Steganos Safe 18

Der Safe ist Ihr sicheres Laufwerk zum Speichern von sensiblen Daten.

Sie verwenden den Safe wie ein Laufwerk Ihres Rechners. Speichern, bearbeiten und löschen Sie dort Dateien. Ist der Safe geschlossen, sind Ihre Daten geschützt. Ohne das Passwort zu kennen, können Unbefugte nichts mit der Safe-Datei anfangen.

Safe einrichten

Schließen Sie Ihre wichtigen Dokumente einfach in den Safe! Dieser Abschnitt erklärt, wie Sie einen "stationären" Safe anlegen. Wenn Sie einen portablen Safe anlegen möchten, den Sie auf einer CD/DVD, einem USB-Stick oder einer externen Festplatte transportieren können, nutzen Sie bitte stattdessen einen "Portable Safe".

Safe erstellen und importieren

Sie können verschiedene Safes anlegen. Um einen neuen Safe zu erstellen, klicken Sie auf "Safe erstellen". Der Assistent führt Sie durch die Einrichtung des Safes. Um einen bereits bestehenden Safe zu importieren, streichen Sie mit der Maus über das Symbol "Safe erstellen" und warten Sie einen Moment, bis ein Menü erscheint. Dort wählen Sie dann bitte "Importieren".

Profi-Tipp: Unter den "Einstellungen" des Safes können Sie auch den "fortgeschrittenen Assistenten" zum Erstellen eines Safes nutzen. Damit können Sie z.B. den Speicherort des Safes verändern (auf eine andere Festplatte z.B.).

Dynamisch wachsende Safes

Wenn Sie einen Safe auf einem lokalen NTFS-Laufwerk erstellen, ist die Option "Laufwerk wächst dynamisch" während der Safe-Erstellung verfügbar. Ein dynamiosch wachsender Safe belegt zunächst nur sehr wenig Speicherplatz auf dem Datenträger und wächst dynamisch mit, wenn Sie Dateien in den Safe kopieren. Auf diese Weise können Sie Speicherplatz einsparen und die Safe-Erstellung deutlich beschleunigen. Hat der Safe die Maximalgröße erreicht, die Sie während der Erstellung festgelegt haben, wächst er nicht mehr weiter.

Bitte beachten: Wachsende Safes können nicht in Verbindung mit Cloud-Speicher genutzt werden. Sobald ein wachsender Safe an einen anderen Speicherort bewegt oder kopiert wird, verliert er seine besonderen Eigenschaften und belegt sofort seine maximale Speicherkapazität, egal, wie groß der eigentliche Safe-Inhalt ist.

Arbeiten mit den Safes

Jedes einzelne der virtuellen Safe-Laufwerke funktioniert wie eine weitere Festplatte in Ihrem Computer: mit dem Unterschied, dass Ihre Daten darin sicher verschlüsselt gespeichert werden.

Sichere Passwörter

Während kryptografische Algorithmen heute aufgrund der Vielzahl von möglichen Schlüsseln unknackbar sind, sind die verwendeten Passworte die Schwachstellen aktueller Verschlüsselungssysteme. Zum einen muss sich in der Regel ein Mensch das Passwort merken, zum anderen muss es eingegeben werden und kann in diesem Moment von anderen Menschen oder Programmen belauscht werden.

Es gibt verschiedene Möglichkeiten, ein Passwort in Erfahrung zu bringen:

Belauschen, ausspähen, erpressen und ergaunern sind geeignet, um unmittelbar in den Besitz eines Passworts zu gelangen. Technische Mittel können davor nur im Einzelfall schützen. Hier ist die Sorgfalt des Anwenders gefragt.

Erraten ist möglich, sobald der Angreifer den Anwender gut genug kennt und die Wahl des Passwortes ohne die notwendige Sorgfalt vorgenommen wurde. Typische Fälle sind hier die Namen von Partnern, Kindern und Haustieren oder auch Telefonnummern und Geburtstage als Passwörter.

Ausprobieren. Der deutsche Sprachschatz umfasst ca. 300.000-500.000 Worte. Der Duden kennt 120.000 Stichworte. Goethe hat ca. 80.000 Worte verwendet. Ein "normaler" Mensch verwendet maximal 10.000 Worte. Die Bildzeitung 1.500. Wird nun ein einfaches Wort als Passwort gewählt, kann es mit hoher Wahrscheinlichkeit mit wenigen hunderttausend Versuchen ermittelt werden, indem einfach alle Worte durchprobiert werden – per Computer kein Problem.

Die im Steganos Safe integrierte Bibliothek warnt Sie vor der Verwendung leicht knackbarer Passwörter, indem das von Ihnen gewählte Passwort mit mehr ale einer halben Million Einträge abgeglichen wird. Es werden ca. 0,3 Sekunden benötigt, um ein Passwort zu überprüfen (P4 3GHz): pro Sekunde also drei Passwörter. Wird also zum Beispiel ein Wort aus der Bildzeitung verwendet, kann dies in maximal 500 Sekunden, also knapp 9 Minuten ermittelt werden, wenn der Angreifer die technischen Möglichkeiten besitzt, diesen Prozess zu automatisieren.

Werden vier beliebige Zeichen (Klein- und Großbuchstaben sowie Ziffern) zufällig kombiniert, ergeben sich daraus mehr als 14 Millionen Möglichkeiten. Das würde auf einem Rechner bereits 57 Tage dauern alle auszuprobieren. Allerdings kann dies mit schnelleren und mehr Rechnern beschleunigt werden. Bei 8 zufälligen Zeichen würden auf einem Rechner mehr als 2 Millionen Jahre benötigt. Dazu würde bereits erhebliche Rechnerkapazität benötigt, um dies auf eine überschaubare Zeit zu reduzieren.

Bei der Auswahl eines Passwortes sollten Sie zunächst bedenken, vor wem Sie sich schützen wollen. Wenn im Privaten Geheimnisse zu schützen sind, sind die Anforderungen an die Passwortqualität geringer als in einem Firmenumfeld, wo Daten möglicherweise vor Mitarbeitern mit IT-Kenntnissen oder Wirtschaftsspionen geschützt werden müssen. Noch deutlich höhere Anforderungen ergeben sich natürlich, wenn Behörden oder Geheimdienste am Zugriff auf Daten gehindert werden sollen.

Es gibt verschiedene Strategien; gute Passwörter zu erzeugen. Die Beste ist die Verwendung eines Passwortgenerators für die Erzeugung eines Passworts, das mindestens aus 10 Zeichen besteht, die wiederum aus mindestens 62 verschiedenen Zeichen (die Klein- und Großbuchstaben des deutschen Alphabets sowie die Ziffern von 0 bis 9) ausgewählt werden. Das Problem hierbei ist natürlich, sich dieses Passwort auch zu merken. Speichern oder Aufschreiben hilft nur begrenzt: Auch wenn ein Passwort-Manager verwendet wird, benötigt man ein sicheres Passwort, um ihn zu öffnen – das sicherste Passwort nützt nichts, wenn es auf einem Zettel neben der Tastatur liegt. Ist das aber nicht der Fall, bietet ein Passwort-Manager eine bequeme und sichere Methode, eine unbegrenzte Zahl an hochsicheren Passwörtern zu erstellen, zu verwalten und auf Wunsch sogar automatisch zu verwenden.

Ein guter Kompromiss zwischen Sicherheit und Gedächtnisleistung sind Abkürzungen für Sätze. EgKzSuGsAfS wäre zum Beispiel das Ergebnis des letzten Satzes. Es sollten ebenfalls mindestens 10 Zeichen herauskommen. Werden dazu noch einzelne Zeichen durch Ziffern oder Sonderzeichen ersetzt, z.B. ‚E' durch "8" (Eight) oder "f" durch ? (Fragezeichen), ergibt sich ein gutes Passwort, das sich leicht herleiten lässt.

Die Erzeugung von zufälligen Passwörtern erhöht die Sicherheit Ihres Passworts. Wenn man sich selbst Passwörter ausdenkt, neigt man dazu, einfache und leicht merkbare Wörter zu verwenden. Der Einsatz einer automatischen Passwortgenerierung garantiert Ihnen, dass das erzeugte Passwort aus einer absolut zufälligen Buchstabenkombination besteht und damit hohe Sicherheit bietet. Durch Konfiguration können Sie bestimmen, was für Elemente Ihr Passwort enthalten soll.

Anzahl der Zeichen

In dem Eingabefeld *Anzahl der Zeichen* bestimmen Sie, wieviel Zeichen das zu generierende Passwort haben wird. Standardmäßig steht der Wert auf sechzehn Zeichen.

kleinbuchstaben verwenden

Ist diese Option aktiviert, so können Kleinbuchstaben im generierten Passwort vorkommen. Standardmäßig ist diese Option aktiviert.

GROSSBUCHSTABEN verwenden

Ist diese Option aktiviert, so können Grossbuchstaben im generierten Passwort vorkommen. Standardmäßig ist diese Option aktiviert.

Zahlen verwenden

Ist diese Option aktiviert, so können Zahlen im generierten Passwort vorkommen. Standardmäßig ist diese Option aktiviert.

Sonderzeichen verwenden

Ist diese Option aktiviert, so können Sonderzeichen im generierten Passwort vorkommen. Standardmäßig ist diese Option deaktiviert, da einige Online-Dienste keine Sonderzeichen zulassen.

Sicherheit des Passwortes mit diesen Eigenschaften

Der Balken sowie die Klartextbewertung zeigen an, wie sicher das gewählte Passwort ist.

Hinweis:
Je mehr Zeichen Sie zulassen, desto sicherer wird das generierte Passwort. Allgemein gilt, dass längere Passwörter sicherer sind.

Wenn Sie die Einstellungen getroffen haben, klicken Sie auf "Weiter". Sie werden dann aufgefordert, die Maus zu bewegen. Mittels dieser Mausbewegungen werden Zufallsdaten für die Schlüsselgenerierung erzeugt.

Erzeugung von Zufallsdaten

Zufallsdaten werden in der Kryptografie für verschiedene Zwecke benötigt. Unter anderem spielen sie eine wichtige Rolle bei der automatischen Generierung von Passwörtern.

Die Generierung von Zufallsdaten ist mit einem Computer nicht ohne weiteres möglich, da für den Prozessor *nichts* zufällig ist. Oftmals wird deshalb spezielle Hardware eingesetzt, um Zufallsdaten zu generieren – beispielsweise durch die Messung von atomarem Zerfall. Eine andere Möglichkeit ist

Interaktion mit dem Benutzer: Bewegen Sie einfach die Maus auf dem dafür vorgesehenen Feld. Da immer leichte Abweichungen in der Mausbewegung auftreten, ist es so möglich, 'echte' Zufallsdaten zu sammeln.

Einige Programme generieren Zufallszahlen aus der aktuellen Systemzeit – diese Vorgehensweise ist für Anwendungsbereiche höchster Sicherheit allerdings nicht geeignet.

Versteckter Safe

Sie können einen Safe in Film- oder Musikdateien sowie in ausführbaren Dateien verstecken. Es handelt sich hierbei nicht um steganographisches Verstecken, bei dem die Daten unsichtbar den Bildinformation beigemischt werden: Die Safe-Datei wird an den Film oder die Musikdatei angehängt. Der Film oder die Musikdatei kann wie gewohnt mit Ihrem bevorzugten Media Player abgespielt werden.

Folgende Formate werden unterstützt:

- mp3
- m4a
- avi
- mpeg
- mov
- exe

Safe verstecken

Zum Verstecken wählen Sie aus dem Kontextmenü eines Safes den Menüpunkt "Verstecken". Folgen Sie dem Assistenten, um eine Trägerdatei auszuwählen, die Ihren Safe beinhalten wird. Nach Abschluß des Assistenten befindet sich der Safe in der Trägerdatei und wird aus dem Hauptmenu von Steganos Safe entfernt. Beachten Sie, dass die Originaldateien zu Ihrer Sicherheit erhalten bleiben. Sie können diese bei Bedarf manuell löschen. Die Option zum Verstecken steht nur bei Safes zur Verfügung, die eine Größe von 3 GB nicht überschreiten.

Versteckten Safe öffnen

Um einen versteckten Safe zu öffnen, klicken Sie bitte auf das entsprechende Icon im Hauptfenster von Steganos Safe. Im nun erscheinenden Assistenten wählen Sie bitte eine Trägerdatei. Nach Eingabe des Passwortes wird der Safe wie gewohnt als Laufwerk unter Windows eingebunden. Der Assistent bleibt solange geöffnet, bis Sie den verstecken Safe wieder schließen möchten.

Bitte beachten Sie: Es handelt sich nicht um ein Verstecken im forensischen Sinne. Mit den entsprechenden Hilfsmitteln kann festgestellt werden, dass sich in einer Trägerdatei ein Safe befindet. Er kann jedoch keinesfalls ohne das richtige Passwort geöffnet werden.

Drag & Drop

Der Safe unterstützt Drag & Drop - Ziehen Sie einfach Dateien oder Ordner auf das Symbol eines Safes im Hauptfenster der Anwendung. Die Dateien werden dann automatisch in den Safe kopiert.

Wenn der Safe zu dem Zeitpunkt geschlossen ist, werden Sie nach dem Passwort gefragt, und er wird automatisch geöffnet. Danach wird der Drag & Drop abgeschlossen.

Safe schließen

Um einen Safe zuschließen, klicken Sie auf das Symbol mit dem geöffneten Safe. Der Safe wird geschlossen und nicht mehr als Laufwerk im Windows Explorer angezeigt. Klicken Sie auf "OK", um die Meldung zu schließen.

Safe öffnen

Um einen Safe zu öffnen, klicken Sie auf das Symbol des gewünschten sicheren Laufwerks.

Geben Sie das Passwort ein und klicken Sie auf "OK".

Schließen Sie die Meldung "Das sichere Laufwerk ist jetzt geöffnet" durch einen Klick auf "OK".

Sie können jetzt mit dem sicheren Laufwerk arbeiten. Dateien, die Sie dort ablegen, werden sofort verschlüsselt.

Im Hauptfenster des Steganos Safe können Sie über das Kontextmenü des geöffneten Safe den Safe im Windows Explorer öffnen.

Nutzung von Safes in der Cloud

Sie haben auch die Möglichkeit, Safes in einem Cloud-Speicher zu erstellen und diese so auf mehreren PCs synchron halten und verwenden zu können. Unterstützt werden Dropbox, Telekom Mediencenter, Microsoft OneDrive und Google Drive.

Cloud-Safe erstellen

Um einen Cloud-Safe zu erstellen, installieren Sie zunächst die Anwendung des jeweiligen Anbieters auf Ihrem PC und verknüpfen diese mit Ihrem Cloud-Account.

Ist der Cloud-Account eingerichtet, klicken Sie im Steganos Safe auf "Safe erstellen", wählen "Erstellen..." und dann "Cloud-Safe". Wählen Sie nun den gewünschten Anbieter aus und erstellen Ihren Safe dann genauso wie einen normalen Safe.

Anschließend wird der Safe mit Ihrem Cloud-Account synchronisiert. Beachten Sie bitte, dass bisher nur Dropbox das selektive Synchronisieren von Änderungen im Safe unterstützt. Nutzen Sie einen anderen Anbieter, wird bei jeder Änderung am Safe die gesamte Safe-Datei erneut synchronisiert. Verwenden Sie

also Telekom-Mediencenter, OneDrive oder Google Drive, bietet es sich an, einen möglichst kleinen Safe zu nutzen, um die Synchronisationszeiten im Rahmen zu halten.

Automatisierung

Dieser Abschnitt richtet sich an fortgeschrittene Benutzer und Administratoren, die mit der Windows-Eingabeaufforderung und der Programmierung von Stapeldateien vertraut sind.

Sie können für gewöhnlich mit der grafischen Benutzeroberfläche des Safe alle notwendigen Operationen ausführen. Falls Sie jedoch nach einem Weg suchen, zum Zweck der Datensicherung und Systemwartung das Öffnen und Schließen von sicheren Laufwerken zu automatisieren, steht Ihnen das Befehlszeilenwerkzeug Safe.exe zur Verfügung.

Hier eine Kurzübersicht der möglichen Befehle:

- **Ein sicheres Laufwerk öffnen:**

  [Pfad_zu]Safe.exe -entry Safe.ToggleDrive.*{Name}* [*Safe.Pass.{Passwort}*]

  Öffnet ein sicheres Laufwerk, falls es geschlossen ist. *{Name}* ist der Name des sicheren Laufwerks. *{Passwort}* ist optional. Wenn das Passwort nicht angegeben wird, wird der Benutzer zur Eingabe des Passworts aufgefordert.

  Vorsicht: Wenn Sie eine Verknüpfung inklusive Passwort anlegen, ist ihr sicheres Laufwerk potentiellen Gefahren ausgesetzt. Denn so kann es auch von jedem, der Ihr Passwort nicht kennt, geöffnet werden.

  Um das Laufwerk mit Passworteingabeaufforderung zu öffnen, geben Sie ein:

  "C:\Program Files (x86)\Steganos Safe 17\Safe.exe" -entry Safe.ToggleDrive.*{Name}* oder "C:\Program Files (x86)\Steganos Privacy Suite 17\Safe.exe" -entry Safe.ToggleDrive.*{Name}* Falls der Name des sicheren Laufwerks Leerzeichen enthält, müssen Sie ihn in Anführungszeichen einfassen.

- **Ein sicheres Laufwerk schließen:**

  [Pfad_zu]Safe.exe -entry Safe.ToggleDrive.*{Name}*

  Schließt ein sicheres Laufwerk, falls es geöffnet ist. *{Name}* ist der Name des sicheren Laufwerks.

  Falls der Name des sicheren Laufwerks Leerzeichen enthält, müssen Sie ihn in Anführungszeichen einfassen.

- **Alle sicheren Laufwerke Schließen:**

  [Pfad_zu]Safe.exe -entry Safe.CloseAll

  Schließt alle sicheren Laufwerke, die gerade geöffnet sind.

Erstellen einer Sicherheitskopie und Einbindung eines vorher erstellten Backups

Wir empfehlen, regelmäßig eine Sicherheitskopie Ihrer Safes auf einem externen Speichermedium zu erstellen. Festplatten können von Datenkorruption betroffen sein, physisch zerstört werden oder einfach mit zunehmendem Alter ihre Funktion verlieren. Sicherheitskopien sind essentiell, um den Verlust Ihrer wichtigen Daten in solchen Fällen zu vermeiden.

Erstellen einer Sicherheitskopie

Um eine Sicherheitskopie erstellen zu können, müssen Sie zunächst den Speicherort Ihrer Safe-Datei feststellen. Rechtsklicken Sie dazu in der Übersicht auf Ihren Safe und wählen "Speicherort ändern". Dies öffnet das Einstellungsmenü des Safes und zeigt dessen derzeitigen Pfad an. Öffnen Sie diesen Pfad im Windows Explorer. Stellen Sie sicher, dass der Safe geschlossen ist und kopieren Sie einfach die Datei mit dem Namen Ihres Safes und der Endung .sle (z.B. mein_safe.sle) auf Ihr Backup-Speichermedium (z.B. eine externe Festplatte).

Ein Backup importieren und wieder einbinden

Um die vorher erstellte Sicherheitskopie einzubinden, wählen Sie einfach in der Menüleiste "Safe" -> "Importieren" aus und geben den Speicherort Ihrer Sicherheitskopie an. Der Safe wird dann in die Hauptübersicht eingebunden und kann dort ganz normal verwendet werden.

Safe-Einstellungen

Um die Einstellungen für ein sicheres Laufwerk aufzurufen, führen Sie den Mauszeiger auf der Seite "Steganos Safe" auf das Symbol für das Laufwerk. Nach einem kurzen Augenblick wird das Kontextmenü angezeigt.

Hier wählen Sie den Menüpunkt "Einstellungen".

Jeder Safe verwendet seine eigene Konfiguration, diese Einstellungen gelten also nur für den jeweiligen Safe, nicht für alle.

Sicheres Laufwerk

Hier können Sie folgende Einstellungen vornehmen:

- Bezeichung
  Ändern Sie hier den Namen Ihres sicheren Laufwerks.
- Sicheres Laufwerk farblich hervorheben
  Verwenden Sie diese Option, um das sichere Laufwerk durch eine Farbmarkierung im Hauptfenster zu kennzeichnen. Mit einem Klick auf die Schaltfläche "Farbe ändern..." können Sie eine beliebige Farbe auswählen. Die Schaltfläche wird erst eingeschaltet, wenn Sie diese Option aktiviert haben.

•Ändern des Laufwerksbuchstabens
Hier können Sie den Laufwerksbuchstaben für Ihr sicheres Laufwerk ändern. Eine Änderung des Laufwerkbuchstabens ist nur bei **geschlossenem** Laufwerk möglich.

•Änderung des Passworts für das sichere Laufwerk
Hier können Sie das Passwort für Ihr sicheres Laufwerk ändern. Eine Änderung des Passworts ist nur bei **geschlossenem** Laufwerk möglich.

•Löschen des sicheren Laufwerks
Um Ihr sicheres Laufwerk zu löschen, klicken Sie auf die Schaltfläche "Löschen...". Bitte beachten Sie, dass das Laufwerk geschlossen sein muss, um gelöscht werden zu können. Nach zweimaliger Sicherheitsabfrage werden Sie darum gebeten, das entsprechende Passwort einzugeben. Erst dann wird die Löschung vollzogen. Das Löschen eines sicheren Laufwerks ist nur bei **geschlossenem** Laufwerk möglich.

•Sicheres Laufwerk als lokales Laufwerk einbinden
Wählen Sie diese Option, falls Sie für das sichere Laufwerk die Indexierung und den Papierkorb verwenden wollen. Das sichere Laufwerk wird dann im Explorer unter Festplatten angezeigt.

•Sicheres Laufwerk als Wechseldatenträger einbinden
Wählen Sie diese Option, falls Sie das sichere Laufwerk ähnlich wie einen USB-Stick verwenden wollen. Das sichere Laufwerk wird dann im Explorer unter Wechseldatenträger angezeigt.

Speicherort

Der Inhalt des sicheren Laufwerks wird in einer SLE-Datei gespeichert. Durch Klicken auf die Schaltfläche "SLE-Datei bewegen" können Sie die Datei an einen neuen Ort verschieben.

Bitte beachten Sie, dass diese Option nur möglich ist, wenn das Laufwerk geschlossen ist.

Ereignisse

Hier legen Sie das Verhalten des sicheren Laufwerks bei bestimmten Ereignissen fest.

•Sicheres Laufwerk automatisch beim Einloggen öffnen
Der Safe wird geöffnet, wenn Sie sich an Ihrem Rechner anmelden und steht danach als sicheres Laufwerk zur Verfügung.

•Sicheres Laufwerk schließen bei Benutzerwechsel, Standbymodus, Ruhezustand und Wechsel zum Bildschirmschoner
Aus Sicherheitsgründen wird der Safe bei Eintritt einer der Bedingungen geschlossen.

•Sicheres Laufwerk automatisch öffnen, wenn das Schlüsselgerät angeschlossen wird
Haben Sie das Passwort zum Safe auf einem USB-Datenträger abgelegt, können Sie über diese Option festlegen, dass der Safe geöffnet wird, wenn der USB-Datenträger angeschlossen wird.

•Sicheres Laufwerk automatisch schließen, wenn das Schlüsselgerät entfernt wird
Haben Sie das Passwort zum Safe auf einem USB-Datenträger abgelegt, können Sie über diese Option festlegen, dass der Safe geschlossen wird, wenn der USB-Datenträger entfernt wird.

Aktionen

Anwendungen können automatisch nach dem Öffnen oder Schließen des sicheren Laufwerks gestartet werden.

•Klicken Sie auf die Schaltfläche "Durchsuchen..." und wählen Sie das Programm oder die Datei aus, die gestartet werden sollen, sobald Sie Ihr sicheres Laufwerk öffnen oder geschlossen haben. *Beispiele:* Ein Bildbearbeitungsprogramm soll starten, wenn Sie das Laufwerk öffnen, in dem Sie Ihre Bilder aufbewahren, oder eine lokales Musikabspielprogramm, wenn Sie auf Ihren Musik-Safe zugreifen.

•Sicheres Laufwerk nach dem Öffnen im Windows Explorer anzeigen
Aktivieren Sie diese Option, damit das sichere Laufwerk nach dem Öffnen automatisch im Windows Explorer angezeigt wird.

Tastaturkürzel

Hier können Sie ein Tastaturkürzel festlegen, mit dem das sichere Laufwerk geöffnet wird.

Dieses Tastaturkürzel funktioniert auch, wenn Steganos Privacy Suite 17 nicht gestartet ist.

Rufen Sie das Tastaturkürzel ein zweites Mal auf, wird das sichere Laufwerk wieder geschlossen.

Postfach-Verschlüsselung

Bitte beachten: Dieses Feature steht nur unter 32-Bit Versionen von Windows zur Verfügung.

Mit der Postfach-Verschlüsselung können Sie E-Mails, Kontakte, Aufgaben und Kalenderdaten von Outlook (ggf. auch anderen unterstützten E-Mail-Programmen) in ein sicheres Laufwerk verschieben und wie gewohnt weiternutzen.

Bitte beachten Sie, daß nur **ein** sicheres Laufwerk für die Postfachverschlüsselung genutzt werden kann. Aus allgemeinen Sicherheitsgründen ist es UNBEDINGT erforderlich, daß Sie eine Datensicherung der Datendatei(en) Ihres E-Mail-Programmes erstellen, bevor Sie mit der Einrichtung der Postfach-Verschlüsselung beginnen.

Die Datendateien für Outlook (*.pst) befinden sich hier:
C:\Dokumente und Einstellungen\[Ihr Benutzername]\Lokale Einstellungen\Anwendungsdaten\Microsoft\Outlook

Frühere Versionen von Outlook legen die Datendatei auch hier ab:
C:\Dokumente und Einstellungen\[Ihr Benutzername]\Anwendungsdaten\Microsoft\Outlook

Bitte stellen Sie sicher, daß Sie ein sicheres Laufwerk von ausreichender Größe erstellen, damit es Ihre Outlook-Datendatei aufnehmen kann. Wir empfehlen: Das Laufwerk sollte mindestens viermal so groß sein, wie die Gesamtgröße Ihrer Outlook-Datendateien.

Beenden Sie Ihr E-Mail-Programm.

Da im Anschluss an die Postfach-Verschlüsselung die Originaldateien gelöscht werden, sollten Sie unbedingt eine Datensicherung durchführen, bevor Sie die Postfach-Verschlüsselung einrichten.

Öffnen Sie den Safe, in dem Sie das Postfach ablegen wollen.

Führen Sie im Bildschirm "Steganos Safe" den Mauszeiger auf das Symbol des sicheren Laufwerks.

Nach wenigen Augenblicken öffnet sich das Kontextmenü. Hier wählen Sie "Einstellungen". Im Bildschirm

"Einstellungen" klicken Sie auf die Schaltfläche "Postfach-Verschlüsselung".

Wählen Sie in der Auswahlliste Ihr E-Mail-Programm und klicken dann auf die Schaltfläche "Einrichten". Die E-Mail-Postfächer, Kontakte, Aufgaben und Kalendereinträge werden jetzt in das sichere Laufwerk kopiert. Anschließend werden die Originaldaten vernichtet.

Klicken Sie in den entsprechenden Meldungen auf "OK".

Bedenken Sie, daß die Größe der Datendatei mit der Zeit anwächst. Zu einem späteren Zeitpunkt können Sie das sicherere Laufwerk ebenfalls aus den Einstellungen in der Größe verändern.

Wenn Sie nun Ihr E-Mail-Programm starten und das sichere Laufwerk mit ihren verschlüsselten Postfachdaten noch nicht geöffnet ist, werden Sie gefragt, ob Sie das verschlüsselte Laufwerk mit dem vorher gewählten Passwort öffnen möchten. Anschließend startet Ihr E-Mail-Programm und Sie können damit wie gewohnt arbeiten.

Anmerkung: Microsoft Outlook 2007 wird nur in der finalen Version unterstützt.

Safe im Safe erstellen

Hier können Sie einen Safe im Safe erstellen. Dieser ist für Außenstehende nicht sichtbar und lässt sich nur mit einem alternativen Passwort bei der Passworteingabe des Hauptsafes öffnen. Beachten Sie bitte, dass diese Funktion nur bei Safes verwendet werden sollte, die mit FAT32 formatiert sind, da bei der Nutzung von NTFS im Safe Datenverlust droht. Die Größe des Safe im Safe ist aus diesem Grund auf maximal 4 GB beschränkt.

Ebenso droht Datenverlust, wenn im äußeren Safe, also dem Safe, der den Safe im Safe beinhaltet, soviel Speicher durch andere Dateien beschrieben wird, dass der Safe im Safe überschrieben wird. Achten Sie also darauf, nie mehr Speicher im äußeren Safe zu verwenden, als nach Erstellung des inneren Safes noch übrig ist.

Beispiel: Sie haben einen Safe mit 4 GB Kapazität und erstellen darin einen Safe im Safe mit 1 GB Kapazität. In diesem Fall sollten Sie nie mehr als 3 GB Daten im äußeren Safe ablegen.