WinSecure 3

für Windows 95/98, Millennium, NT 4, Windows 2000 und Windows XP

Administrationshandbuch

WinSecure 3
Professional Edition

Inhaltsverzeichnis

1. Allgemeines

Perfekte Sicherheit für Windows PC

- *Schützt vor Manipulation des PC*
- *Schützt vor Installation von unerwünschten Anwendungen*
- *Schützt vor Viren und Trojanern*
- *Schützt Ihre Daten durch "on the fly" Verschlüsselung*

1.1. Einleitung

Herzlichen Glückwunsch zum Erwerb der WinSecure® 3 PROFESSIONAL Edition!

Sie haben mit dem Kauf von WinSecure® 3 PROFESSIONAL Edition eine gute Wahl getroffen und damit eines der sichersten und effizientesten Desktop Sicherungssysteme für die Windows Betriebssystempalette von Microsoft überhaupt erworben.

Die Sicherheitssystematik von WinSecure beruht auf einer speziell entwickelten und patentierten Technologie - der **RBCD Technologie**. Es ist genau diese Technologie, die es Ihnen jetzt erstmals ermöglicht, Ihr IT System mit einem **dynamischen** Schutz zu sichern. Sie haben mit Hilfe von WinSecure® jetzt die Möglichkeit, u.a. Dateien und Verzeichnisse unabhängig von Ihrem Herkunftsort und unabhängig davon, ob bestimmte Dateien (z.B. Viren) schon bekannt sind oder existieren mit den entsprechenden Sicherheitsattributen zu versehen.

Sicherheit ist auch eine Grundsatzfrage.

Aufgrund der unglaublichen Vielzahl von verschiedenen Viren, Hackerangriffe und sonstigen Sicherheitsproblematiken stellte sich die Frage, ob mit den herkömmlichen Sicherheitsansätzen den rasend schnellen Verbreitungsmechanismen z.B. über Internet und den nicht fassbaren Variationsmöglichkeiten ein effiziente und zugleich verlässliche Absicherung heute und in Zukunft überhaupt noch möglich sein wird.

Der Sicherheitsansatz von WinSecure ist anders!

WinSecure bietet Ihnen als Administrator erstmals die Möglichkeit, den PC komplett seiner Funktionen zu berauben um dann im zweiten Schritt nur die explizit benötigten Ressourcen wie Applikationen, Laufwerke, Systemeinstellungsmöglichkeiten, Verzeichnisse und Dateien benutzerspezifisch wieder freizugeben.

Die ist neu - aber sehr wirkungsvoll!

Wir sind sicher, dass Ihnen WinSecure 3 Professional Edition ein effizienter und zuverlässiger Helfer bei der Absicherung Ihres IT Systems sein kann.

Übrigens - Sicherheit ist nicht nur sehr komplex sondern auch sehr dynamisch. Deswegen wollen wir Ihnen gemeinsam mit unseren WinSecure® Fachhandelspartnern und WinSecure Systempartnern bei Bedarf auch mit Rat und Tat zur Verfügung stehen.

Lieber sicher - mit WinSecure®!

Was ist neu in der Version 3?

Die neue WinSecure® PROFESSIONAL Edition ist eine grundlegend überarbeitete Version des Vorgängers WinSecure 98. WinSecure® 3 bietet nun optional einen eigenen Anmeldedialog und viele Assistenten, die Ihnen die Arbeit erleichtern. Bei der Entwicklung haben wir sehr viel Wert darauf gelegt, dass WinSecure® in nahezu jeder Umgebung problemlos funktioniert. So haben wir den Schutz von der Prozessebene nahezu komplett auf die Datenträgerebene gelegt. Dies ermöglicht WinSecure® in der jetzigen Ausgabe alle Aktivitäten, die auf gesperrte Dateien zugreifen, zu protokollieren.

Eine weitere Neuigkeit ist das Kryptomodul, mit dem Sie verschlüsselte Datenbereiche auf Ihrer Festplatte anlegen können. Dies verhindert zuverlässig den Zugriff auf sensible Daten auf der Festplatte auch für den Fall, dass der Datenträger in einen anderen PC eingebaut und dann über ein anderes Betriebssystem gelesen wird. Das Kryptomodul bietet im Gegensatz zu vielen anderen Programmen den Vorteil, dass nur mit erfolgreicher Anmeldung an WinSecure® der geschützte Datenbereich zugänglich gemacht wird. Als Verschlüsselungsmethoden werden Blowfish, 3DES und WSummer angeboten. Andere Verschlüsselungsmethoden können auf Wunsch integriert werden.

Außerdem ist das Einrichten von mehreren Benutzern mit der aktuellen Version von WinSecure® so einfach wie nie zuvor. Import- und Exportdateien sowie Profilverzeichnisse gehören der Vergangenheit an. Alle benutzerspezifischen Dateien werden auf dem WinSecure® Server in einer Datenbank verschlüsselt gespeichert (128-Bit-Verschlüsselung).

Der Administrator hat die Möglichkeit, sämtliche Laufwerke, Verzeichnisse und Dateien mit speziellen Dateiattributen zu versehen, um damit sein System individuell abzusichern.

Für den Schulungsbetrieb stehen spezielle Funktionen zur Verfügung, die es z.B. erlauben, alle Rechner mit denselben Einstellungen automatisch und zentral gesteuert hoch- und herunterzufahren.

Und last but not least haben wir eine eigene Notfallroutine eingebaut - für den Fall, dass Sie sich komplett ausschließen oder das System von fehlerhafter Hard- oder Software zum Absturz gebracht wird.

Wozu braucht man WinSecure®

Seitdem die Kosten für Hardware immer weiter gefallen sind und die „Überfrachtung“ der Standardbetriebssysteme mit jedem nur erdenklichen Feature zu einer für den normalen Benutzer fast nicht mehr überschaubaren Komplexität geführt hat, ist die Gesamtkostenbetrachtung (TCO, Total Cost of Ownership) zu einem festen Begriff geworden. **Weniger ist mehr**, gilt hierbei in beinahe jeder Umgebung. Da dieser Wunsch jedoch der Strategie der meisten Softwarehäuser, mit immer mehr Funktionen immer breitere Käuferschichten ansprechen zu können, leider nicht gerecht werden kann, stellt sich die Frage, ob eine individuelle Beschränkung der Möglichkeiten des einzelnen Benutzers nicht nur zur Kosteneinsparung, sondern auch zu einer Erhöhung des Bedienkomforts sowie vor allem zu einer deutlichen Erhöhung der Sicherheit führt.

Genau auf diese Bedürfnisse ausgerichtet wurde WinSecure® entwickelt. WinSecure® bietet damit erstmals die Möglichkeit, die Funktionen eines PC nach Belieben einzuschränken. Die Zielsetzung, die WinSecure® verfolgt, ist einfach:

1. *Senkung der TCO,*
2. *Verbesserung des Kosten/Nutzen Verhältnisses und*
3. *Erhöhung der Sicherheit von IT Systemen.*

Dabei deckt WinSecure® PROFESSIONAL Edition die Betriebssysteme Windows 95, Windows 98, Windows Millennium, Windows NT4, Windows 2000 und Windows XP ab.

WinSecure® stellt dabei keine Konkurrenz zum ZAK oder der Management-Konsole von Windows 2000 von Microsoft dar. Vielmehr ist WinSecure® eine benutzerfreundliche Ergänzung dieser Tools und deckt die wichtigsten fehlenden Sicherheitsfunktionen zuverlässig ab. Dabei erfordert WinSecure® weitaus weniger Fachkenntnisse und stellt die gesamte Sicherheits-Funktionalität sowohl im Netzwerk als auch jedem Einzel-PC zur Verfügung. Das ZAK kann beim Einsatz von WinSecure® als Ergänzung dienen, z.B. um die Funktionen der Office-Produktfamilie auf Applikationsebene einzuschränken.

Die Kernfunktionen von WinSecure® bieten:

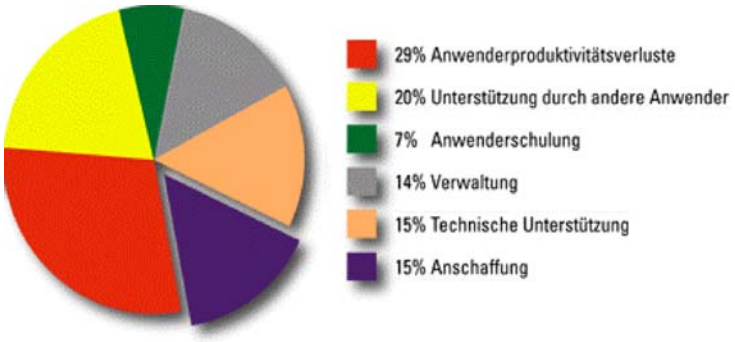
1. *die Einschränkung des Arbeitsplatzes auf das für die Arbeit notwendige Maß,*
2. *die Verhinderung der Installation sowie des Starts von unerwünschten Anwendungen,*
3. *den Schutz des Betriebssystems vor Manipulation*
4. *eine einfache Methode, wandernde Benutzerprofile zu generieren und*
5. *Daten verschlüsselt auf der Festplatte abzulegen.*

Als technische Besonderheit bietet WinSecure® die Möglichkeit, die Sicherheit ohne Neuanmeldung am System unter jedem beliebigen Benutzerkonto zu aktivieren bzw. zu deaktivieren. Damit sind Softwareinstallationen wesentlich einfacher. Auch Programme, die sich in der Registrierungsdatenbank des lokalen Benutzers eintragen, sind voll funktionsfähig.

Wie bei allen Sicherheitsprodukten - egal ob Firewall, Virenschutz oder WinSecure® - werden auch bei der Weiterentwicklung von WinSecure® neu auftretende Sicherheitsrisiken berücksichtigt. Die WinSecure® Website bietet deshalb unter www.WinSecure.de nicht nur die Möglichkeit, Sicherheitslücken zu melden, sondern stellt auch entsprechende Updates bei Bedarf zur Verfügung.

1.2. Die Kostenbetrachtung

In einer Studie der Gartner Group vom Mai 1997 wurde folgende Aufteilung der Kosten eines Desktop-PCs ermittelt:



WinSecure® kann kostensparend wirksam auf die Anwenderproduktivitätsverluste, die Unterstützung durch andere Anwender, die Verwaltung und die technische Unterstützung und damit auf nahezu 80% der Kosten, die ein PC verursacht, Einfluss nehmen.

Nachfolgend einige Beispiele für häufig entstehende Kosten durch unbeabsichtigte Aktionen der Benutzer:

- *Nicht genehmigte Installationen von Software aus dem Internet, von Kollegen oder von privaten PC. Dies führt häufig zu Problemen und ist oft illegal – **die Geschäftsführung haftet persönlich**!*
- *Nicht durchdachte Veränderung der Systemsteuerung oder Registrierdatenbank, z.B. durch die Verwendung der Netzwerkadresse eines Kollegen, "um auch ins Internet zu kommen" ohne den Administrator zu fragen;*
- *die "Verseuchung" des PC oder Netzwerkes mit Viren durch Software installationen oder das Ausführen diverser Programme von CD-ROM, eMail Attachments usw.;*
- *"Anpassungen" der Systemeinstellungen wie z.B. Farben, Hintergründe und Drucker; dies führt häufig zur Unbrauchbarkeit des PC;*
- *Benutzung von diversen Programmen und Spielen, die für die berufliche Arbeit nicht benötigt werden;*
- *Der "Forscherdrang" und die menschliche Neugierde, also z.B. solche Fragen wie: "Was kann wohl unter "Systemsteuerung-Hardware" eingestellt werden?" oder Aussagen wie: "Mein PC hat kein Bild mehr, seit ich die Auflösung auf 1600x1200 Bildpunkte hochgestellt habe".*

Mit WinSecure® lassen sich unerwünschte Aktionen dieser Art einfach und zuverlässig verhindern. Die Produktivität von Windows-Systemen erhöht sich spürbar, indem die Funktionalität der Systeme auf das vom Benutzer benötigte Maß zugeschnitten wird.

Die Bedienfreundlichkeit von WinSecure® gestattet dadurch den Einsatz von WinSecure® auch bei kleineren Firmen und bei Privatpersonen, die keine Profis im Umgang mit der Systemsicherheit von Windows sind.

Ohne auf die Leistungsfähigkeit und Flexibilität eines Standard Windows PC verzichten zu müssen, lassen sich durch den Einsatz von WinSecure® die heute angestrebten Vorteile eines Netz-PC (Thin Client) erreichen.

1.3. Auswirkung auf die Gesamtkosten eines EDV-Arbeitsplatzes (TCO)

WinSecure® kann Einfluß auf bis zu 80% der TCO nehmen. Dies sind im einzelnen:

Anwenderproduktivitätsverluste: Durch die Verhinderung der Ausführung „nicht zugelassener“ Programme sowie deren Installation und die Beschränkung der Einstellungsmöglichkeiten des Arbeitsplatzes lassen sich diese Verluste auf unter 5% drücken.

Unterstützung durch andere Anwender: Der bekannte „Hey Joe-Effekt“ (Hey Joe, kannst du mir mal helfen?) lässt sich mit WinSecure® zwar nicht eliminieren, jedoch auf zugelassene Aktionen beschränken. Da sich über die Hälfte solcher Fälle jedoch auf Programme bezieht, die der Anwender gar nicht benötigt, oder Einstellungen korrigieren hilft, die der Anwender gar nicht ändern hätte sollen, kann durch den Einsatz von WinSecure® diese Verlustgröße auf unter 10% beschränkt werden.

Schulung: Durch den reduzierten Funktionsumfang des Betriebssystems und der Anzahl von Programmen lässt sich auch der Schulungsaufwand für die Windows-Betriebssystemfamilie gering halten. Das Einsparpotential liegt hier immerhin noch bei 2-3%.

Verwaltung: Die Kosten für die Verwaltung lassen sich mit WinSecure® durch zentralisierbare Konfiguration und Unterstützung des Softwaremanagements um ca. 5% senken.

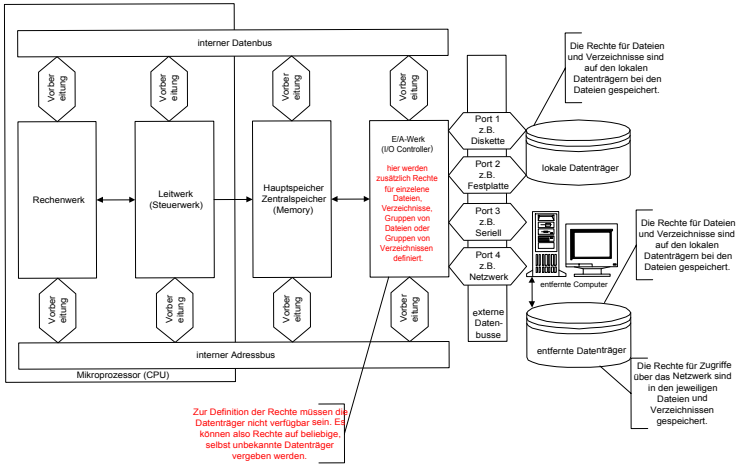
Technische Unterstützung: Eine weitere enorme Kostensenkungsmöglichkeit bietet WinSecure® im Bereich Help-Desk. Viele Neuinstallationen, Korrekturen am Betriebssystem und den Systemeinstellungen können mit WinSecure® verhindert werden. Neuinstallationen sind mit WinSecure® sehr viel einfacher. Hierdurch können die Supportkosten um über 10% gesenkt werden.

2. Die Wirkungsweise von WinSecure®

WinSecure® besitzt einen Filetreiber der es mit einer patentierten Technologie ermöglicht, Zugriffe auf Laufwerke, Ordner und Dateien zu kontrollieren. Der Filetreiber sitzt dabei zwischen dem Betriebssystem und den Speichermedien wie Festplatten, Diskettenlaufwerke, CD-Roms und Netzlaufwerken. Dabei muss jeder Zugriff auf die Speichermedien den WinSecure®-Filetreiber passieren und dieser entscheidet, ob ein Filezugriff erlaubt ist oder nicht. Jedem Laufwerk, jedem Verzeichnis und jeder Datei können zudem spezielle Attribute zugewiesen werden, die den Zugriff auf jene einschränken. Diese Attribute sind z.B: nicht öffnen, nicht lesen, nicht schreiben, nicht löschen, nicht umbenennen, verstecken, nicht erstellen.

Die Grundkonfiguration des Filetreibers ist so eingestellt, dass die bereits installierten Programme erlaubt sind. Bei der Installation für jeden Benutzer kann dann festgelegt werden welche Programme dem jeweiligen Benutzer zur Verfügung stehen.

Nachfolgendes Schaubild zeigt die prinzipielle Funktionsweise.



WinSecure® ist es dadurch möglich, intern eine Liste von „Zugelassenen Dateien“ zu führen. Das hat zur Folge, dass keine Programme zur Ausführung gebracht werden können, die nicht vom Administrator explizit zugelassen wurden. Im Reiter „**Hilfe**“ können Sie sich ein Treiberabbild erstellen lassen. In diesem Treiberabbild können Sie die Handlungsvorschriften des Filetreibers leicht erkennen.

Die Sicherheits-Philosophie hinter WinSecure®

Lassen Sie uns WinSecure® zuerst mit den heute verfügbaren Virenscannern vergleichen. Ein Virenscanner arbeitet nach dem Prinzip „Die Welt ist so lange gut, bis meine Definitionen sagen, dass etwas schlecht ist“. Mit diesem Verhalten ist zwar die maximale Funktionalität gegeben, jedoch haben Viren wie „I LOVE YOU“ bewiesen, dass diese Methode der enormen Geschwindigkeit und den Variationsmöglichkeiten, die u.a. das Internet ermöglicht, nicht gewachsen sind.

WinSecure® dreht dieses Prinzip exakt um und arbeitet nach dem Motto „Die ganze Welt ist so lange schlecht, bis auf Ausnahmefälle die mir mein Administrator mitteilt.“

Auch Dateirechte, die Sie vielleicht von NTFS oder aus UNIX kennen, werden den geänderten Anforderungen alleine nicht mehr gerecht, da der Benutzer immer Bereiche auf seiner Festplatte benötigt, auf denen er vollen Zugriff besitzt. Mit WinSecure® können diese Bereiche gezielt eingegrenzt werden, da WinSecure® Rechte nach Masken vergeben kann.

Die RBCD-Technologie

Rights **B**y **C**losest **D**efinition oder übersetzt „**Rechte nach genauester Definition**“ ist eine patentierte Technologie, die es WinSecure® ermöglicht, trotz der unendlichen Menge von Dateien, die auf einem PC, im Internet oder als Email Anhang vorkommen können, einfach und zuverlässig für genau definierte Sicherheit zu sorgen!

Damit der Filetreiber seine Arbeit verrichten kann, benötigt er zwei Dinge.

1. Zum einen Regeln, die die Sicherheit definieren und

2. zum anderen eine Sortierung für die gegebenen Regeln, falls mehr als eine Regel auf eine bestimmte Datei oder ein bestimmtes Verzeichnis zutreffen.

Regeln sind Vorschriften, die der Filetreiber entsprechend in die Tat umsetzt.

Nachfolgend zwei Beispiele für solche Regeln.

* | *.EXE - DelFi MkFi OpFi RenFi WrFi RdFi ChAt SubFo DenEx Hide

C:\PROGRAMME\FRITZ! | FRIVER32.EXE - DelFi RenFi ChAt

Eine Regel besteht immer aus dem Pfad, der Maske und den vergebenen Rechten.

Da ein Objekt immer nur eine Sicherheitsbeschreibung besitzen kann, muß für den Fall, dass mehr als eine Regel auf ein Objekt zutrifft eine Sortierung bzw. eine Hierarchie eingeführt werden. WinSecure® nimmt in diesem Fall immer die Regel, die das Objekt am genauesten beschreibt. Hierfür werden die Zeichen für Pfad und Maske addiert.

Ein Beispiel für die Datei c:\programme\wawi\fibu.exe soll uns zeigen wie die Sortierung funktioniert. Das Attribut „/s“ soll anzeigen, dass die Regel auch für alle Unterverzeichnisse gilt.

Pfad	Maske	Attribut	Ergebniss
*	*.*	/s	Treffer 1
*	*.exe	/s	Treffer 2
*	fibu.exe	/s	Treffer 3
c:\programme	*.*	/s	Treffer 4
c:\programme	fibu.exe		Kein Treffer (/s fehlt!)
c:\programme\wawi	*.*		Treffer 5
c:\programme\wawi	fibu.exe		Treffer 6

Die genaueste Beschreibung für unser Objekt finden wir im Treffer 6, der zur Beschreibung des Pfades und der Maske exakt 25 Zeichen benötigt hat. Damit liegt er vor Treffer 5 (20), Treffer 4 (15), Treffer 3 (9), Treffer 2 (6) und Treffer 1 (4).

Zum einfacheren Verständnis der Funktionsweise erstellen Sie einfach wie beschrieben ein Treiberabbild. Danach vergleichen Sie dieses Abbild (Abbild.txt) mit den vergebenen Rechten auf Dateien und Verzeichnisse. Daraus ersehen Sie, welche Sicherheitseinstellung für welche Dateien und für welche Verzeichnisse im Moment gelten.

3. Installation und Konfiguration

!! ACHTUNG !!

WinSecure® ist ein Sicherheitsprodukt und greift tief in Ihr System ein! Bitte lesen Sie auf jeden Fall diese Dokumentation VOR der Installation!

3.1. Vor der Installation

WinSecure® PROFESSIONAL Edition ist ein leistungsfähiges Sicherheitstool, das zum Absichern von Windows 95, Windows 98, Millennium, Windows NT4, Windows 2000 und Windows XP dient.

WinSecure® verhindert, dass Systemeinstellungen geändert, Dateien gelöscht oder nicht gewünschte Programme gestartet werden können. Zusätzlich können Daten verschlüsselt abgelegt werden.

Dabei ist WinSecure® einfach zu bedienen und leicht verständlich. Es ist wichtig, dass Sie sich vor der Implementierung der Sicherheitseinstellungen mit diesem Handbuch vertraut machen. Sie finden in diesem Handbuch alle wichtigen Einstellungen für Ihren PC,

- *um ein höchstmögliches Sicherheitsniveau zu erhalten.*
- *um Administratoren unnötige und vermeidbare Neuinstallationen ersparen zu können,*
- *um Geschäftsführer aus der Haftung für illegale Softwareinstallationen zu befreien*
- *um sensible Daten vor Manipulation, Diebstahl und Vernichtung zuverlässig und trotzdem praktikabel zu schützen*

!! Achtung !!

Um mit WinSecure® einen wirksamen Schutz zu erhalten, sollten Sie vor der Installation von WinSecure® einige Einstellungen an Ihrem PC überprüfen und gegebenenfalls korrigieren!

- *Als Bootreihenfolge des PC muss das Laufwerk C vor dem Laufwerk A und dem CD-ROM eingestellt sein. Sie können diese Parameter im BIOS-SETUP des PC einstellen. Nähere Informationen enthält das Handbuch zu Ihrem PC.*
- *Das BIOS-SETUP Ihres PC **muss** durch ein Kennwort geschützt werden. Anderenfalls können Anwender die Bootreihenfolge ändern und den PC mit einer Bootdiskette oder CD-ROM ungeschützt starten.*

- *Machen Sie nach Möglichkeit ein Backup Ihres PC! Dies sollten Sie grundsätzlich vor jeder Installation neuer Systemkomponenten tun.*
- *Überlegen Sie gut, welche Programme Sie im geschützten Modus zulassen wollen. Programme wie z.B. FDISK (formatiert die Festplatte) sollten jedenfalls nicht erlaubt sein.*
- ***Bei Windows 95:** Um die Systemeinstellungen vor der Installation zu sichern, verwenden Sie unter Windows 95 hierzu das Programm ERU, das auf der Windows 95-CD im Verzeichnis \other\misc\eru zu finden ist. Da ERU i.d.R. nicht alle Dateien auf eine Diskette schreiben kann, sollten Sie die Systemdateien in ein eigenes Verzeichnis "C:\ERD" sichern lassen und danach die Dateiattribute für den Schutz der ERD-Dateien setzen.*
- ***Bei Windows 98**: Unter Windows 98 führen Sie den Befehl "Scanregw" unter Start-Ausführen aus. Die Registrierungsdatenbank wird automatisch in das Verzeichnis \Windows\Sysbckup gesichert.*
- ***Bei Windows NT und Windows 2000**: Bei Windows NT, Windows 2000 und Windows XP erstellen Sie eine Notfalldiskette. Nähere Information zur Erstellung der Notfallsicherung gibt Ihnen das Handbuch zu Ihrem Betriebssystem.*

Wiederherstellen der ursprünglichen Konfiguration:

In seltenen Fällen kann es vorkommen, dass Ihr PC nicht mehr fehlerfrei startet. Dies kann z.B. der Fall sein, wenn durch die Installation anderer Programme systemwichtige Dateien von WinSecure® überschrieben oder gelöscht werden.

Bei Windows 95: Wenn das System unter Windows 95 nicht mehr startet, müssen Sie im Setup des PC die Bootreihenfolge auf A, C umstellen und danach von der Notfalldiskette booten. Wechseln Sie nach dem Systemstart in das Verzeichnis C:\ERD und starten Sie das Programm ERD.EXE.

Bei Windows 98 geben Sie nach dem Start mit der Notfalldiskette den Befehl "Scanreg /restore" ein.

Nach einer eventuellen Wiederherstellung müssen Sie WinSecure® erneut installieren.

Wenn Sie sich mit dem Benutzer "WSADMIN" anmelden, wird WinSecure® prinzipiell nicht gestartet. Versuchen Sie daher bei Schwierigkeiten, sich zuerst als "WSADMIN" einzuloggen. Die allermeisten Probleme werden Sie auf diese Art und Weise beheben können.

Unter Windows NT, Windows 2000 und Windows XP stellen Sie das System mit der Notfalldiskette wieder her.

Mit der Installation von WinSecure® anerkennen Sie den Lizenzvertrag, den Sie am Ende des Benutzerhandbuches finden.

Mit dem Erwerb von WinSecure® haben Sie auch eine Lizenzdiskette erhalten. Das Registrierungsformular auf der Lizenzdiskette sollten Sie ausgefüllt an die Faxnummer 07352-9222-90 zurückfaxen oder das Formular ausdrucken und an die Datapol GmbH einsenden. Sie werden dann automatisch über alle Neuerungen informiert.

Bewahren Sie die Lizenzdiskette gut auf. Sie ist der Nachweis und die Voraussetzung für den Erwerb eines Updates auf kommende Betriebssysteme.

Wenn Sie alle Vorbereitungen getroffen haben, können Sie mit der Installation von WinSecure® beginnen.

3.2. Installation

!! ACHTUNG !!

WinSecure® ist ein Sicherheitsprodukt und greift tief in Ihr System ein! Bitte lesen Sie auf jeden Fall diese Dokumentation VOR der Installation!

3.2.1. Erstinstallation von WinSecure®

Setup und Einrichtung

Die WinSecure® PROFESSIONAL Edition ist für den professionellen Einsatz gedacht. Mit seinem speziellen Filetreiber bietet es viele Möglichkeiten, sämtliche Dateien Ihres Computers zu beeinflussen. Es ist damit möglich, jede beliebige Datei zu sperren. Bei unsachgemäßem Gebrauch kann dies dazu führen, dass Ihr Betriebssystem nicht mehr ordnungsgemäß funktioniert.

Deshalb sollten Sie die erweiterten Einstellungen im Reiter “Dateirechte” von WinSecure® PROFESSIONAL nur dann benutzen, wenn Sie mit Windows und den eingesetzten Applikationen vertraut sind und genau wissen, was Ihre Änderungen bewirken können.

Für den Fall, dass Sie versehentlich zuviel gesperrt haben, können Sie sich entweder unter dem Benutzernamen “WSADMIN” anmelden oder Sie schalten den PC aus und wieder ein. WinSecure® meldet, dass es nicht korrekt beendet wurde und fragt Sie, ob der nächste Start im Scanmode durchgeführt werden soll. Bei einem Start im Scanmode wird die Sicherheit nicht aktiviert. Näheres hierzu finden Sie im Abschnitt **Liste häufig gestellter Fragen.**

Doch nun zur Installation und der nachfolgenden Konfiguration von WinSecure® PROFESSIONAL Edition:

WinSecure® PROFESSIONAL Edition besteht aus zwei Komponenten:

1. *WinSecure® Client und*
2. *WinSecure® Server*

Auf jedem Arbeitsplatz (Clients) wird die Clientkomponente installiert und auf einem Rechner (bestehender Server oder extra WinSecure Server) in Ihrem Netzwerk wird die Serverkomponente installiert.

Was müssen Sie installieren:

Einzel-PC nicht vernetzt und Notebooks:

Installieren Sie lediglich den WinSecure® Client. Auf der Installations-CD finden Sie zwei Clients.

1. *einen für die Betriebssysteme Windows 95, Windows 98 und Windows Millennium und*
2. *einen für die Betriebssysteme Windows NT4, Windows 2000 und Windows XP.*

Mehrere PC im Netzwerk, die gemeinsame Einstellungen verwenden sollen:

Installieren Sie

1. *zuerst den WinSecure® Server und*
2. *anschließend die WinSecure® Clients.*

3.2.2. Installation des WinSecure®-Servers

Installation des WinSecure® Servers:

Auf der WinSecure® CD befinden sich zwei Versionen des WinSecure®-Servers.

1. *Die “**NT-Dienst Version**” installiert sich als Dienst und ist damit auch dann lauffähig, wenn kein Benutzer an Windows angemeldet ist. Diese Version des Servers können Sie nur auf solchen Computern installieren, auf denen Windows NT, Windows 2000 oder Windows XP als Betriebssystem genutzt wird.*

*2. Die "**Anwendungs-Version**" des WinSecure®-Servers läuft auf allen Windows-Betriebssystemen ab Windows 95 und ist eine Anwendung. D.h. am Computer muss ein Benutzer angemeldet sein, damit der WinSecure®-Server gestartet werden kann.*

Alle Benutzereinstellungen werden auf dem zentralen Server (Serverkomponente) gespeichert.

Die Serverkomponente von WinSecure® sollten Sie auf einem PC installieren, der zu jeder Zeit läuft.

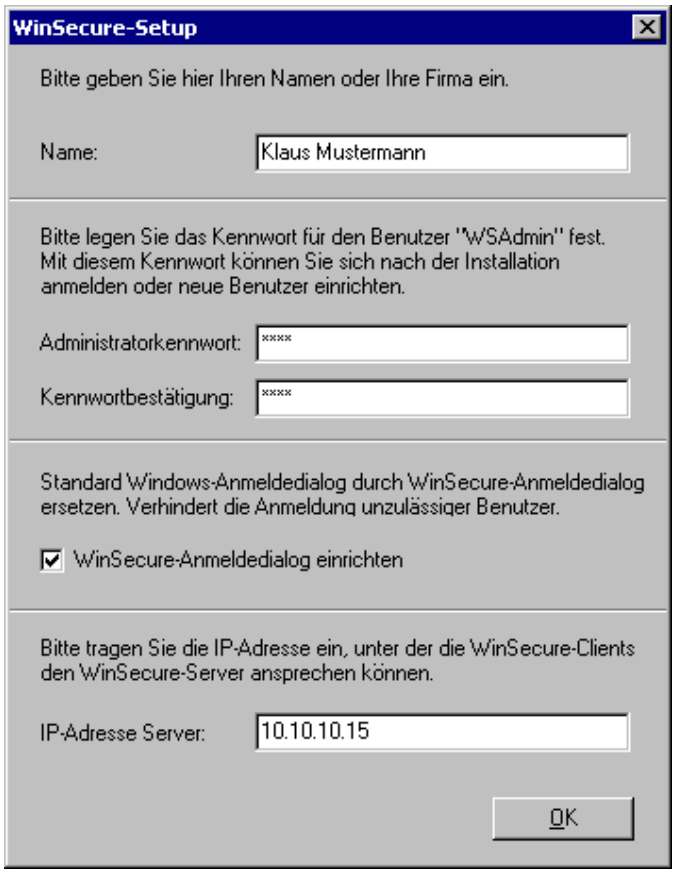
Dies kann ein PC unter Windows 95, Windows 98, Millennium, Windows NT4, Windows 2000 oder Windows XP sein. Der WinSecure® Server hat keinerlei Sicherheitsfunktionen und kann daher bedenkenlos auch auf einem Server oder Domänencontroller installiert werden. Die Serverkomponente bedient lediglich eine Datenbank in der die Benutzerdaten verschlüsselt gespeichert werden. Bei jeder Anmeldung eines Benutzers holt der WinSecure® Client abhängig vom Benutzernamen die Daten vom WinSecure® Server und stellt entsprechend die Sicherheitseinstellungen für den sich anmeldenden Benutzer her. Dies hat den Vorteil, dass sich jeder Benutzer an einem beliebigen Computer anmelden kann und trotzdem immer seine persönlichen Sicherheitseinstellungen bekommt. Sie können die WinSecure® PROFESSIONAL Edition auf einem Rechner ohne Netzwerk installieren. In diesem Fall verwendet der Client den integrierten WinSecure® Server und speichert dann alle Informationen lokal.

Wenn Sie einen WinSecure® Server einsetzen möchten, installieren Sie bitte diesen zuerst. Wählen Sie dazu auf der Installations-CD die Datei "Setup.exe" und starten Sie diese. Bei der Installation des Servers sind folgende Dinge zu beachten:

- *Der Server sollte eine nicht wechselnde IP-Adresse besitzen (verwenden Sie kein DHCP). Die Clients finden ansonsten den WinSecure® Server nicht mehr.*
- *Der Server muss über das TCP/IP Netzwerk alle Clients erreichen können.*
- *Der WinSecure® Server kann nur auf einem Windows Betriebssystem instal liert werden. Wenn Sie in Ihrem Netzwerk einen Novell-Server verwenden, müssen Sie den WinSecure® Server auf einem beliebigen anderen Compu ter mit einem Windows Betriebssystem installieren.*

Bei der Installation des WinSecure® Servers werden Sie aufgefordert, die IP-Adresse des Servers und einen Namen für die zu registrierende Person oder Firma einzugeben. Des weiteren müssen Sie mit einer Checkbox wählen, ob Sie den Anmeldebildschirm von WinSecure® verwenden wollen oder nicht. Der Anmeldebildschirm von WinSecure® gibt an eventuell nachfolgende Logon Provider (Domänen- oder Novell-Anmeldung) die eingegebenen Daten weiter. Bei richtiger Konfiguration brauchen deshalb Benutzername und Passwort nur ein mal eingegeben werden.

Wenn man nicht den mitgelieferten Anmeldedialog verwendet, wird die WinSecure®-Sicherheit für den Benutzer hergestellt, der an Windows angemeldet wird. Wenn ein Benutzer die Anmeldung abbricht (ist unter Windows95,98,ME möglich) oder existiert der unter Windows angemeldete Benutzer in der WinSecure® Benutzerdatenbank nicht, bekommt der angemeldete Benutzer die Standardeinschränkungen der Gruppe "WSSTANDARD". Lesen Sie hierzu mehr in dem speziellen Kapitel über die Benutzergruppe WSSTANDARD.



Mit dem Button "**Client-Setup-Datei erstellen**" können Sie veranlassen, dass Sie beim Installieren der Clients keinen Registrierungsnamen, kein Administratorpasswort und keine IP-Adresse für den Server eingeben müssen.

Sie können auch die Installation der Clients komplett automatisieren, indem Sie eine Client-Setup-Datei erstellen und dem Setup-Programm von WinSecure® den Schalter "/verysilent" übergeben.

Dazu gehen Sie wie folgt vor:

Speichern Sie die Setup.exe für die Installation der Clients in einem Verzeichnis und geben Sie dieses Verzeichnis frei. Die Client-Setup-Datei müssen Sie nun in dieses Verzeichnis speichern.

Wenn Sie sowohl Windows 95, Windows 98, Millennium, als auch Windows NT4, Windows 2000 oder Windows XP Clients installieren wollen, müssen Sie die Client-Setup-Datei zweimal erstellen.

Näheres finden Sie im Abschnitt Installation des WinSecure®-Clients.

Nach der Installation des WinSecure® Servers können Sie diesen aus dem Startmenü heraus starten. Die Dienste-Version unter Windows NT, Windows 2000 und Windows XP können Sie in der Systemsteuerung unter Dienste starten und beenden.

Beachten Sie, dass Sie den WinSecure® Server nur mit dem Konto und Kennwort eines Administrators beenden können.

Bei jedem Neustart des Server-PC wird der WinSecure® Server automatisch gestartet!

!! ACHTUNG !!

Treten bei der Installation des WinSecure® Servers Fehlermeldungen auf, so haben Sie wahrscheinlich keine oder veraltete ODBC-Komponenten für den Zugriff auf die Datenbank installiert. Installieren Sie in diesem Fall die neuesten ODBC-Treiber von der WebSite http://www.microsoft.com/data.

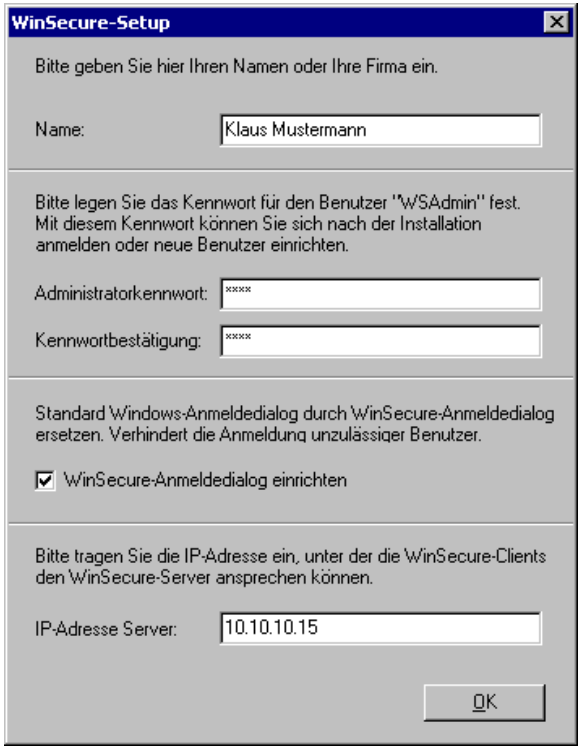
Das Setup Programm versucht ebenfalls die ODBC-Komponenten zu installieren, so dass dieser Fall nur sehr selten und nur dann auftreten sollte, wenn die ODBC-Installation beschädigt oder inkompatibel ist.

3.2.3. Installation des WinSecure®-Clients

Schließen Sie alle offenen Anwendungen. Legen Sie die CD-ROM ein, das Installationsprogramm sollte nun automatisch gestartet werden. Wenn das Programm nicht automatisch gestartet wird, starten Sie auf der CD die Datei SETUP.EXE über den Windows-Explorer im Verzeichnis des verwendeten Betriebssystems. Beachten Sie, dass Sie für Windows95/98/ME ein anderes Setup benötigen als für Windows NT, Windows 2000 und Windows XP.

Während der Installation werden Sie aufgefordert, den Registrierungsnamen und das Administratorpasswort einzugeben. Merken Sie sich das eingegebene Administratorkennwort. Es gibt keine Möglichkeit, ein vergessenes Kennwort wieder sichtbar oder rückgängig zu machen.

Schalten Sie während der Installation den PC nicht aus und unterbrechen Sie die Installation nicht!



Automatisierung der Installation von Clients

Wenn Sie wie im Abschnitt “Installation des WinSecure®-Servers” beschrieben eine Client-Setup-Datei erstellt haben, können Sie die Installation der Clients automatisieren.

Ein entsprechendes Anmeldescript sieht in etwa wie folgt aus:

```
if exist C:\WINDOWS\WIN.com goto Win9598ME
goto NT
:Win9598ME
if exist C:\PROGRA~1\DATAPOL\WINSEC~1\Winsec~1.exe goto weiter
f:\install\W9598ME\setup.exe /verysilent
:NT
if exist C:\PROGRA~1\DATAPOL\WINSEC~1\Winsec~1.exe goto weiter
f:\install\NT_W2K\setup.exe /verysilent
:weiter
```

ACHTUNG: Sie sollten die Setup Antwortdatei so auf dem Server speichern, dass normale Anwender darauf keinen Zugriff erhalten, da ansonsten unbefugte PC zu Ihrem WinSecure®-Verbund hinzugefügt werden können.

!! ACHTUNG !!

Treten bei der Installation des WinSecure® Servers Fehlermeldungen auf, so haben Sie wahrscheinlich keine oder veraltete ODBC-Komponenten für den Zugriff auf die Datenbank installiert. Installieren Sie in diesem Fall die neuesten ODBC-Treiber von der WebSite http://www.microsoft.com/data.

Das Setup Programm versucht ebenfalls die ODBC-Komponenten zu installieren, so dass dieser Fall nur sehr selten und nur dann auftreten sollte, wenn die ODBC-Installation beschädigt oder inkompatibel ist.

3.2.4. Lizenzierung der Software

Ihrer WinSecure® Software liegt eine Lizenzdiskette bei. Auf dieser Diskette befinden sich die von Ihnen gekauften Lizenzen in der entsprechenden Anzahl.

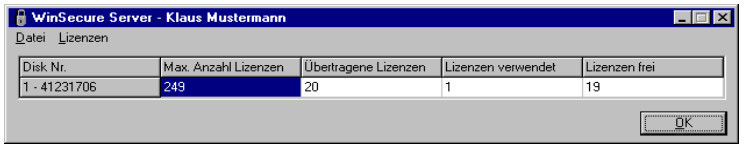
Sie benötigen für jeden PC auf dem WinSecure® installiert wird eine separate Lizenz. Diese Lizenz müssen Sie von der Diskette auf den Rechner übertragen.

Grundsätzlich können bei der Lizenzierung zwei Fälle auftreten:

1. *ein WinSecure® Client, der zusammen mit einem WinSecure® Server in einem Netzwerk läuft.*
2. *ein WinSecure® Client, der ohne WinSecure® Server läuft.*

Lizenzierung im Netzwerk in dem ein WinSecure® Server vorhanden ist:

Im Normalfall betreiben Sie Ihre Rechner in einem Netzwerk in dem Sie einen WinSecure® Server installiert haben. Starten Sie zum Übertragen der Lizenzen nun den WinSecure® Server. Im Menüpunkt “Lizenzen” finden Sie den Auswahlpunkt “Lizenzen übertragen”. Wenn Sie diesen auswählen, werden Sie aufgefordert, die Lizenzdiskette ins Diskettenlaufwerk einzulegen. Sie können nun auswählen, wie viele Lizenzen Sie auf den WinSecure® Server übertragen wollen. Ist dies erfolgreich geschehen, sieht dies in der Administration des Servers in etwa so aus:



In dem Feld “Disk Nr.” finden Sie die Seriennummer der Diskette. Im Feld “Max. Anzahl Lizenzen” finden Sie die Anzahl der Lizenzen auf der Diskette. Im Feld “Übertragene Lizenzen” finden Sie die Anzahl der Lizenzen, die Sie von der Diskette auf den WinSecure® Server übertragen haben. Im Feld “Lizenzen verwendet” sehen Sie, dass von den 20 übertragenen Lizenzen bereits eine an einen Client vergeben wurde und im Feld “Lizenzen frei” sehen Sie, dass noch 19 Lizenzen zur Verfügung stehen.

!! Achtung !!

Übertragen Sie die die Zahlenkombination im Feld “Disk Nr.” manuell auf das Etikett der Lizenzdiskette! Sie können die Lizenzen des Servers später ausschließlich auf diese Diskette zurückübertragen!

Sie können Ihre Lizenzen auf mehrere Server verteilen und mit der gleichen Lizenzdiskette Server und Stand-Alone-Clients lizenzieren.

Natürlich können Sie zu einem späteren Zeitpunkt weitere Lizenzen zu einem WinSecure®-Server hinzufügen. Erwerben Sie dazu einfach eine weitere Lizenzdiskette und übertragen Sie die Lizenzen der zweiten Lizenzdiskette ebenfalls auf den WinSecure® Server. Die Gesamtanzahl aller verfügbaren Lizenzen ergibt sich dann aus der Summe der einzelnen Lizenzen aller verwendeter Lizenzdisketten.

Beim Start eines WinSecure® Client wird zuerst überprüft, ob dieser eine Lizenz besitzt. Wenn dies nicht der Fall ist, versucht der Client den Server zu erreichen und von diesem dann automatisch eine Lizenz abzubuchen.

Beim Starten des Clients meldet sich dieser, sollte er noch keine Lizenz zugeteilt bekommen haben.

Wenn Sie die Administration von WinSecure® öffnen, sehen Sie im Reiter "**Information**" im unteren rechten Bereich, ob der entsprechende Client bereits lizenziert wurde oder nicht.

Lizenzierung auf Einzelplatzrechnern, die ohne WinSecure® Server arbeiten:

In manchen Fällen kann es vorkommen, dass Sie einen oder mehrere WinSecure® Clients ohne WinSecure® Server betreiben. Vielleicht haben Sie kein Netzwerk oder aber Sie möchten WinSecure® auf einem Notebook oder Stand-alone PC installieren.

In diesen Fällen wird WinSecure® den bei jedem Client integrierten Server benutzen. Um den integrierten Server verwenden zu können sollten Sie sicherstellen, dass in der Administrationsoberfläche im Reiter "**Benutzer**" im Feld "**IP-Adresse**" der Wert " **127.0.0.1**" steht. Diese IP-Adresse bezeichnet die Loopbackadresse und beschreibt den lokalen Rechner. Wenn dies richtig eingestellt ist und Sie WinSecure® starten, meldet sich WinSecure® mit der Information, dass noch keine Lizenz vorliegt. Beim Drücken von "OK" werden Sie dann aufgefordert, eine Lizenzdiskette einzulegen. Der Client holt sich dann seine Lizenz direkt von der Diskette.

Wichtig:

Sie brauchen KEINE Netzwerkkarte oder TCP/IP auf einem Einzelplatz zu installieren um einen Stand-alone-Client von WinSecure® zu nutzen.

Zurückschreiben von Lizenzen an den WinSecure® Server oder auf die Lizenzdiskette:

Es ist generell auch möglich, vergebene Lizenzen wieder zurückzuschreiben. Beim öffnen der WinSecure® Administration finden Sie im Reiter "**Information**" einen Button "**Lizenz zurückschreiben**". Wenn Sie diesen betätigen, versucht der WinSecure® Client seine Lizenz entweder auf den WinSecure® Server oder auf die Lizenzdiskette zurück zu schreiben falls der Client den lokalen WinSecure®-Server nutzt.

Diesen Vorgang können Sie nutzen, wenn Sie einen bereits lizenzierten PC gegen ein neues Gerät austauschen wollen.

Zurückschreiben von Lizenzen des WinSecure® Servers auf die Lizenzdiskette:

Auch ein Server-PC muss einmal ausgetauscht werden! Um Ihnen eine möglichst flexible Lizenzverwaltung zu ermöglichen können Sie deshalb einige oder alle Lizenzen, die auf dem WinSecure® Server noch vorrätig sind auf die Lizenzdiskette zurückschreiben.

Verlust der Lizenzdiskette!

Die WinSecure® Lizenzdiskette ist kopiergeschützt und intern markiert! Bewahren Sie ihre Lizenzdiskette deshalb sorgfältig auf. Verlorene Lizenzdisketten werden NICHT ersetzt!

Beschädigung der Lizenzdiskette!

Die WinSecure® Lizenzdiskette ist kopiergeschützt und intern markiert! Jeder Versuch die Lizenzdiskette zu kopieren kann zur Beschädigung führen. Natürlich kann eine Lizenzdiskette auch durch häufigen Gebrauch oder einen Fabrikationsfehler beschädigt werden.

In diesem Fall senden Sie die Originalrechnung, eine Kopie der Lizenzkarte und die beschädigte Lizenzdiskette an:

Datapol GmbH
Lizenzverwaltung
Bahnhofstraße 24
88416 Ochsenhausen

Bis zu 7 Tagen nach Kauf des Produktes erhalten Sie eine neue Lizenzdiskette kostenlos zugesandt. Danach erheben wir eine Bearbeitungsgebühr von • 19,00.

3.2.5. *Konfiguration des WinSecure®-Clients*

Wenn Sie die Installation beendet und den Rechner neu gestartet haben, wird künftig bei jedem Start unter Windows die WinSecure® Anmeldung erscheinen (falls konfiguriert):

!! ACHTUNG !!

Solange Sie noch keine WinSecure Benutzer erstellt oder importiert haben können Sie sich ausschliesslich mit dem Benutzernamen "WSADMIN" anmelden!

Bei der WinSecure® Anmeldung wird der eingegebene Benutzername und das Benutzerkennwort an die bereits bestehenden Anmeldedialoge von Windows oder Novell weitergegeben.

Falls der WinSecure® Benutzername und das WinSecure® Kennwort mit dem früheren Benutzernamen und dem früheren Passwort der Windows oder Novell Anmeldung übereinstimmt wird der Zutritt sofort gewährt, ohne Benutzer und Kennwort in der Windows oder Novell Anmeldung noch einmal eingeben zu müssen. Sie werden also durch die WinSecure® Anmeldung automatisch an Ihrem Windows- oder Novell Client mit angemeldet.

Falls Sie in WinSecure® und Windows/Novell verschiedene Benutzernamen und Passwörter haben, müssen Sie sich nach der WinSecure® Anmeldung an Ihrem Windows/Novell Anmeldedialog noch einmal anmelden. Bitte beachten Sie, dass Sie in diesem Fall die richtigen Benutzernamen und Passwortkombinationen eingeben:

1. *Anmeldung an WinSecure®: WinSecure® Benutzernamen und WinSecure® Passwort eingeben*
2. *Anmeldung an Windows/Novell: bestehende und vorher benutzte Benutzer namen und Passwörter eingeben*

Wenn Sie also mehrere Anmeldedialoge haben, ist es sinnvoll, wenn Sie den entsprechenden Benutzern bei den unterschiedlichen Anmeldedialogen dieselben Passwörter vergeben.

Beim ersten Start von WinSecure® wird standardmäßig der Benutzer "**WSADMIN**" erscheinen. Das Benutzerkennwort für den Benutzer "**WSADMIN**" haben Sie während des Installationsvorgangs festgelegt.

Wenn Sie sich als "**WSADMIN**" am System anmelden, wird WinSecure® prinzipiell nicht gestartet. Es ist als Benutzer "WSADMIN" auch nicht möglich, WinSecure® aus dem Startmenü heraus zu starten. Lediglich die Administration von WinSecure® kann mit diesem Benutzer geöffnet werden. Benutzen Sie diesen Benutzer also dann, wenn es irgendwelche Probleme mit einem der anderen, von Ihnen angelegten Benutzern gibt. Zum Deaktivieren der Sicherheit benutzen Sie ebenfalls den Benutzer "WSADMIN" bzw. einen anderen Benutzer, der in WinSecure® Administratorrechte hat.

Im Folgenden werden wir den Benutzerassistenten zum Anlegen von Benutzern erläutern. Wir stellen uns die konkrete Situation vor, dass Sie einen oder mehrere neue Benutzer anlegen wollen. Sie möchten, dass die unterschiedlichen Benutzer unterschiedliche Programme ausführen dürfen. Sie haben beispielsweise Microsoft Office installiert und möchten, dass die Benutzer unterschiedliche Programme in Office benutzen dürfen.

Beispiel:

1. *Ihrem ersten Benutzer genügt es, wenn er Word und Excel ausführen darf (Benutzer Thomas).*
2. *dem zweiten Benutzer möchten Sie lediglich erlauben, dass er den Internet Explorer und Outlook benutzen kann.*

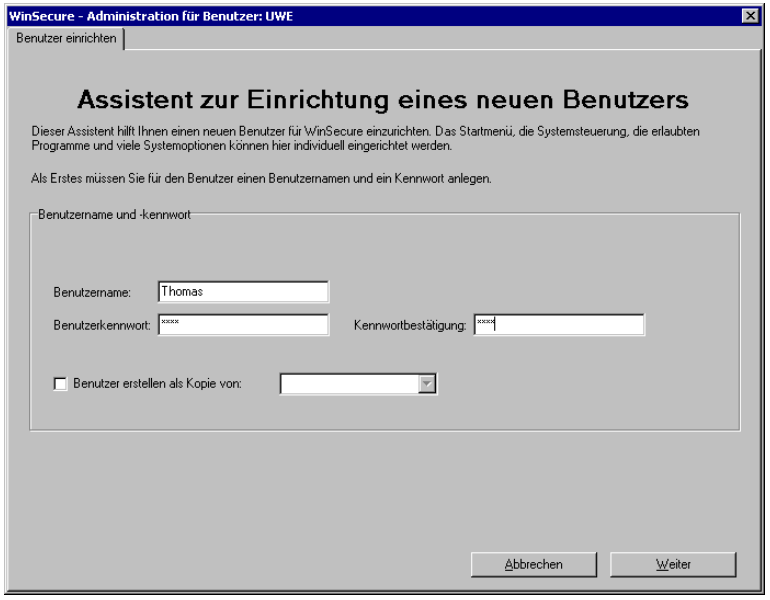
Als Administrator von WinSecure® wollen Sie selbst natürlich den kompletten Rechner benutzen und verwenden daher beim Anmelden an der WinSecure®-Anmeldung den Benutzer "WSADMIN" mit dem von Ihnen gewählten Kennwort. Alternativ dazu können Sie sich auch mit Ihrem eigenen Passwort anmelden und das dann erscheinende Schloss mit dem Passwort öffnen. Sie müssen Ihren Benutzer dann allerdings vorher bei den WinSecure® Administratoren hinzugefügt haben. Bei geöffnetem, grünen Schloss steht Ihnen der Rechner ohne Einschränkungen zur Verfügung.

Beginnen wir also nun mit dem Anlegen des Benutzers “Thomas”.

Anlegen eines für WinSecure® neuen Benutzers:

1. *Deaktivieren Sie die Sicherheit falls diese aktiviert ist (rotes Schloss) oder*
2. *melden Sie sich als Benutzer “WSADMIN” an WinSecure® an.*
3. *starten Sie aus dem Startmenü die Administration von WinSecure®.*
4. *Wenn Sie die Administration geöffnet haben, öffnen Sie den Reiter “Benut zer”.*
5. *Klicken Sie dann den Button “WinSecure® Benutzerverwaltung” an. Dort fin den Sie unten rechts den Button “Neuer Benutzer” zum Anlegen eines neuen Benutzers. Jetzt wird der Benutzerassistent zum Anlegen eines neuen Benut zers gestartet. Sie können beliebig viele Benutzer auf einem PC mit einer Lizenz von WinSecure® einrichten.*

Die erste Eingabemaske sieht folgendermaßen aus:



Geben Sie nun nach Ihrer Wahl den Benutzernamen und das Benutzerkennwort des neuen Benutzers ein. Wenn Sie auf Ihrem Computer schon bestehende Benutzer angelegt haben, können Sie dieselben Benutzer und auch dieselben Benutzerkennwörter verwenden. Bestätigen Sie unter “Kennwortbestätigung” das angegebene Benutzerkennwort und klicken Sie danach auf “Weiter”.

Wenn Sie bereits einen Benutzer mit gleichen oder ähnlichen Einstellungen erstellt haben, so können Sie den neuen Benutzer als Kopie eines bereits existierenden Benutzers erstellen.

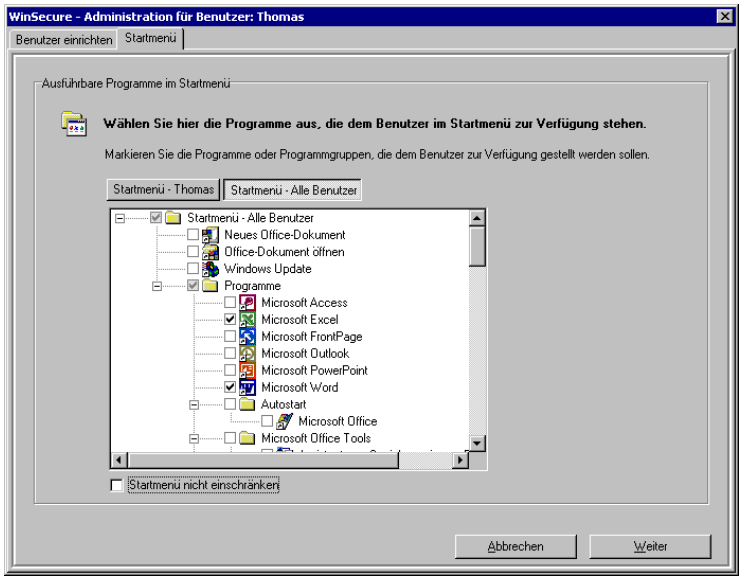
Für den gerade angegebenen Benutzer wird jetzt ein neuer WinSecure® Benutzer mit dem speziellen WinSecure® Benutzerprofil angelegt.

Falls Sie unter Windows 95/98/ME in der Systemsteuerung unter dem Eintrag “Kennwörter” im Reiter “Benutzerprofile” den Auswahlpunkt “**Benutzer können die Vorgaben und Desktopeinstellungen ändern**” ausgewählt haben, wird unter C:\windows\profiles auch in Windows ein neues Profil angelegt.

Falls Sie den Punkt “**Für alle Benutzer dieses Computers gelten dieselben Vorgaben und Desktop-Einstellungen**” im selben Reiter ausgewählt haben, wird in Windows kein neues Benutzerprofil für den angelegten Benutzer eingerichtet.

Jetzt erscheint der Reiter “Startmenü” im Benutzerassistent. WinSecure® liest nun automatisch alle auf der Festplatte installierten Programme aus und zeigt diese dann in einem Verzeichnisbaum hier für den eben angelegten Benutzer “Thomas” an. Bei einem umfangreichem Startmenü kann dies etwas dauern - wir bitten um ein wenig Geduld. Ebenfalls wechselt der Benutzer in der Kopfleiste vom bisherigen Benutzer “Uwe” auf den momentan in Bearbeitung befindlichen Benutzer “Thomas”.

Soll das Startmenü für den angelegten Benutzer nicht eingeschränkt werden, kann durch Anhaken von “Startmenü nicht einschränken” das normale Startmenü angezeigt werden.



ACHTUNG:

Da zur Zeit der Anzeige des Startmenüs für den neuen Benutzer das Startmenü noch nicht existiert (das Startmenü wird erst bei der ersten Anmeldung des neuen Benutzers angelegt) versucht WinSecure® das Startmenü des neuen Benutzers möglichst exakt darzustellen. Nicht immer jedoch entspricht dieses Startmenü dem endgültigen Startmenü des Benutzers.

Sie können jetzt mit der Maus und den Scrollbars am rechten und unteren Bildschirmrand zu den entsprechenden Programmen navigieren und diese dann mit der Maus **anklicken** und damit "**zulassen**". Alle Programme, die Sie in diesem Menü auswählen, erscheinen dann später im Startmenü für diesen Benutzer. Wollten Sie also für den Benutzer "Thomas" Word und Excel zulassen, so müssen Sie sowohl Word als auch Excel hier anhaken. Wenn Sie auf den Button "Weiter" klicken, kommen Sie in das nächste Menü.

Alle **nicht angehakten** Programme stehen dem Benutzer **nicht zur Verfügung**. Dies gilt selbst dann, wenn der Benutzer versucht, ein Programm über Umwege (beispielsweise aus dem Windows-Explorer) zu starten. WinSecure® überwacht im laufenden Betrieb alle Programmstarts und unterbindet den Start von nicht autorisierten Programmen oder Programmteilen unabhängig davon, von wo sie aufgerufen wurden. Daher ist es fast unmöglich, sich mit aktiviertem WinSecure® einen Virus einzufangen, weil dieser nicht auf dem System ausgeführt werden kann.

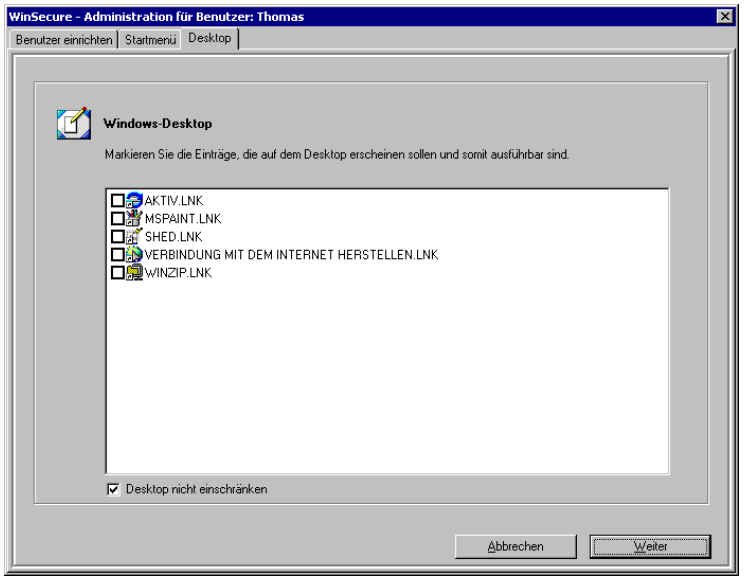
Unter Windows NT und Windows 2000 verfügt jeder Benutzer über ein geteiltes Startmenü.

Sein persönliches Startmenü sowie das Startmenü für alle Benutzer werden dabei zu einer Anzeige addiert. WinSecure® bietet Ihnen die Möglichkeit beide Menüs entsprechend zu kontrollieren.

Im Reiter "Desktop" können Sie für den Benutzer "Thomas" festlegen, welche Desktop Icons er auf dem Desktop sehen darf. Sowohl Word als auch Excel hat auf dem Desktop keine Linkdateien gespeichert, deshalb werden diese beiden hier nicht angezeigt.

Sollen alle auf dem Desktop befindlichen Linkdateien angezeigt werden, kann die Checkbox "Desktop nicht einschränken" angehakt werden.

ACHTUNG: Die Icons die im Desktop "Alle Benutzer" gespeichert sind werden hier nicht angezeigt.



Im Reiter "**Systemsteuerung**" können Sie festlegen, welche Systemsteuerungselemente unter "Start / Einstellungen / Systemsteuerung" für den jeweiligen Benutzer zugelassen sind. Standardmäßig werden keine Zugriffe auf die Systemsteuerung erlaubt.

Wir empfehlen hier, nur in Ausnahmefällen Systemeinstellungsmöglichkeiten freizugeben. Im Normalfall ist dies eine typische Aufgabe des Administrators und nicht der Benutzer.

Unter Windows Millennium und Windows 2000 werden Sie einige Optionen doppelt vorfinden. Dies ist kein Fehler in WinSecure® sondern von Microsoft so in Windows Millennium und Windows 2000 eingebaut worden. Sie können die Optionen, die als Symbol ein Schloss besitzen in den meisten Fällen ignorieren. Da aber auch Drittanbieter diese zweite Technologie nutzen können müssen Sie eventuell Einträge doppelt aktivieren.

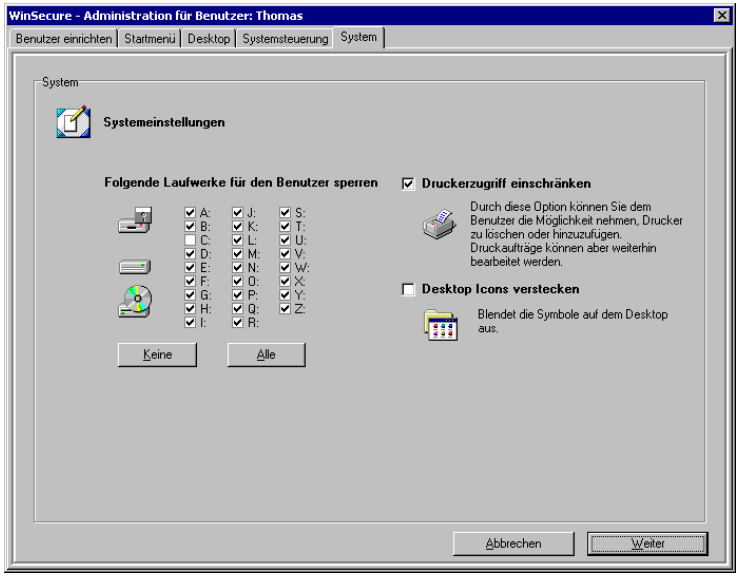
Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie bitte auf "Weiter".

Danach kommen Sie in den Reiter "**System**". Hier sehen Sie in der linken Bildschirmhälfte die Laufwerke wie zum Beispiel das Diskettenlaufwerk, das Festplattenlaufwerk und die Netzlaufwerke aufgeführt. In der rechten Bildschirmhälfte können Sie den Druckerzugriff einschränken, die Desktop Icons verstecken und den DOS-Modus beim Beenden von Windows verbieten (nicht notwendig unter Windows NT, Windows 2000 und Windows XP).

In unserer Beispielkonfiguration sehen Sie, dass alle Laufwerke (ausgenommen Laufwerk C) durch das Anhaken gesperrt wurden. Sie können damit den Zugriff beispielsweise auf das Diskettenlaufwerk oder das CD-Rom- Laufwerk unterbinden.

Das Zugriffsverbot gilt auch für Zugriffsversuche aus dem Internet oder über das Netzwerk!

Wenn Sie das Laufwerk “C” anhaken, also ihre lokale Festplatte, werden die Daten lediglich versteckt und nicht gesperrt.



Alle gesperrten Laufwerke sind aus keiner Applikation mehr zugreifbar. Außerdem besteht auch nicht die Möglichkeit, auf Laufwerke mittels eines “File Open”-Dialoges einer Anwendung heraus zu gelangen. Die Laufwerke sind gesperrt, als wären sie physikalisch nicht vorhanden. Die einzige Ausnahme macht das Systemlaufwerk, auf dem Windows installiert ist. (i.d.R. das Laufwerk “C”). Dieses wird von WinSecure® beim Anhaken lediglich versteckt. Der Grund dafür ist, dass das Betriebssystem Schreibzugriff auf bestimmte Dateien haben muss. Beim kompletten Sperren dieses Laufwerkes würde das Betriebssystem nicht mehr funktionieren.

Sie können allerdings selbst Laufwerke, Verzeichnisse und Dateien mit speziellen Attributen versehen um Ihr System sicherer zu machen. Mehr dazu erfahren Sie im Kapitel “Der Reiter Dateien zulassen”.

!! Achtung !!

Haben Sie zum Beispiel Microsoft Word auf der Festplatte D:\ installiert und dieses Laufwerk gesperrt, Word jedoch im Startmenü zugelassen, so werden Sie beim Start von Word viele Fehlermeldungen erhalten, da z.B. die Normal.dot oder auch die Programmerweiterungen von Word nicht mehr verfügbar sind!

Unter Windows NT, Windows 2000 und Windows XP können alle Wechseldatenträger (Floppy, CD-ROM, ZIP...) derzeit (02/2002) nur hier gesperrt werden. Wenn diese Laufwerke nicht komplett gesperrt sind, können beliebige Programme von ihnen gestartet werden.

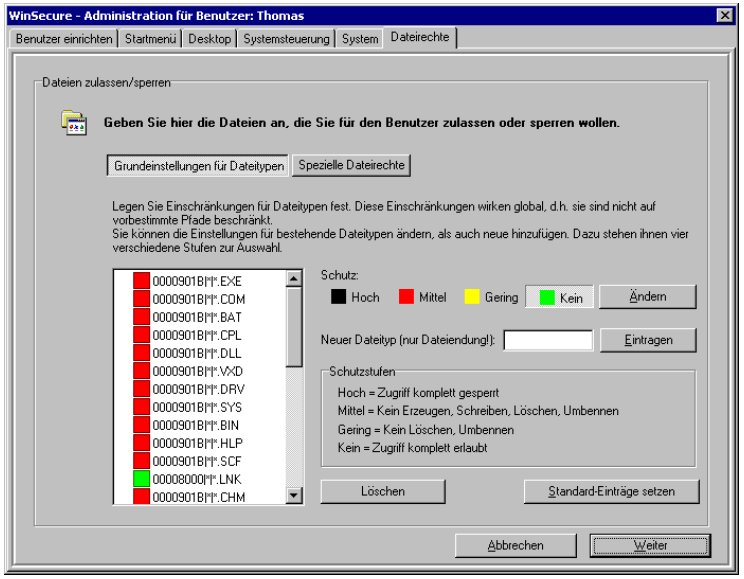
Auf der rechten Bildschirmhälfte können Sie durch Anhaken den Druckerzugriff einschränken. Dem Benutzer ist dann nur noch erlaubt, auf dem für ihn eingestellten Drucker zu drucken. Er hat zwar die Möglichkeiten, Einstellungen am Drucker zu ändern, jedoch fehlt ihm die Möglichkeit, neue Druckertreiber zu installieren oder aber auch vorhandene Druckertreiber zu löschen.

Mit der Funktion “**Desktop Icons verstecken**” werden für den angelegten Benutzer alle Desktop Icons bei aktivierter Sicherheit ausgeblendet. Damit steht dem Benutzer nur noch das Startmenü zum Starten von Programmen zur Verfügung. Wenn Sie dieses Häkchen nicht gesetzt haben, können Sie im Reiter “Desktop” diejenigen Icons definieren, die dieser Benutzer sehen soll.

Mit der Auswahlbox “**MS-DOS Modus sperren**” kann unterbunden werden, dass der Benutzer beim Herunterfahren des Rechners in den DOS-Modus gelangt. (nur Windows 95/98/ME).

Wenn Sie mit den Einstellungen fertig sind, klicken Sie bitte auf “Weiter”.

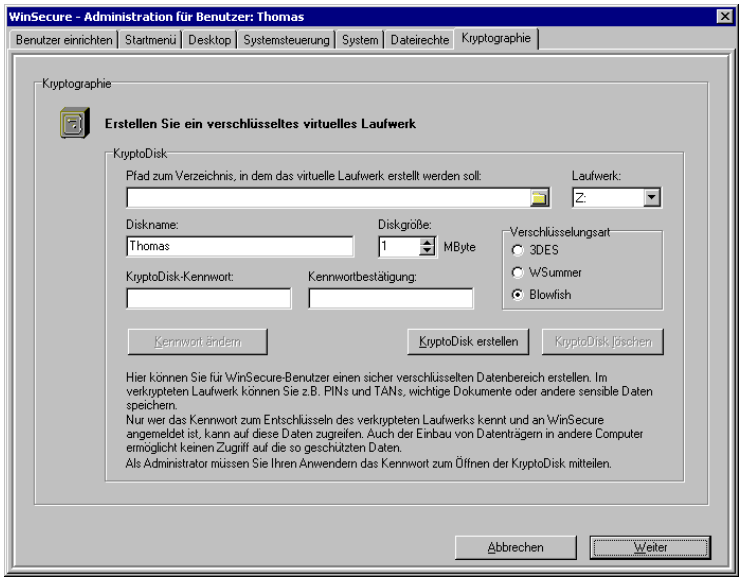
Damit kommen Sie zum Menüeintrag “Dateirechte”. Hier sind die generellen Rechte für Dateitypen geregelt. Die Grundeinstellungen sind so gewählt, dass die auf dem System existierenden Dateien laufen können und zugelassen sind, es können allerdings keine neuen Dateien gespeichert werden. Zu Beginn kann man diesen Reiter überspringen, eventuell müssen Sie aber später hier noch Eintragungen vornehmen.



Im Normalfall sind an dieser Stelle noch keine Einstellungen nötig. Klicken Sie deshalb auf “Weiter”.

Sie gelangen jetzt in den Reiter “**Kryptographie**”. In diesem Reiter können Sie ein verschlüsseltes Datenlaufwerk für den angelegten Benutzer einrichten. Verwenden Sie das selbst angelegte Verschlüsselungslaufwerk wie ein ganz normales Laufwerk, indem Sie Dateien abspeichern oder bereits gespeicherte Daten weiter verarbeiten. Dabei werden - *für den Anwender unsichtbar* - alle Daten verschlüsselt auf der Festplatte abgelegt. Dies hat den Vorteil, dass niemand, außer dem Benutzer selbst die Daten einsehen kann. Die gilt auch dann, wenn die lokale Festplatte in einen anderen Rechner eingebaut wird.

Für unser Beispiel brauchen wir allerdings kein Kryptolaufwerk und machen deshalb weiter. Im Kapitel “**Der Reiter Kryptographie**” wird genau beschrieben, wie Sie ein Kryptolaufwerk einrichten.



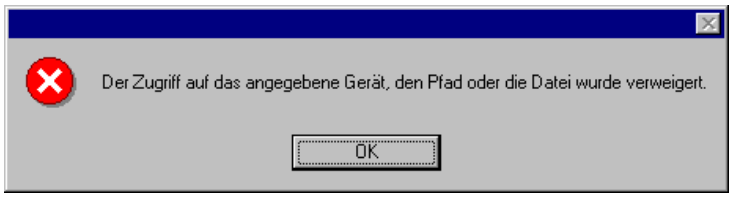
Damit kommen Sie dann schon zum Abschluss der Konfiguration für den Benutzer “Thomas”.

Sie haben nun die Möglichkeit, einen weiteren Benutzer anzulegen. Der Ablauf für das Anlegen eines weiteren Benutzers ist analog. Wenn Sie “Fertigstellen” wählen, kommen Sie wieder in den Reiter “Benutzer” in der Administration.

Falls Sie den neu angelegten Benutzer testen wollen, müssen Sie den gerade angemeldeten Benutzer abmelden. Geben Sie dann bei der Anmeldemaske den Benutzernamen das Kennwort des zu testenden Benutzers ein. Nach dem Starvorgang erscheint in der Taskleiste dann ein geschlossenes (rotes) Schloss, welches anfangs kurz blinkt. Damit wird dem Benutzer angezeigt, dass er mit aktivierter Sicherheit von WinSecure® arbeitet.

Sie werden feststellen, dass sich das Startmenü auf nur die Programme reduziert hat, welche Sie bei der Konfiguration zugelassen haben.

Wenn Sie entweder vom Desktop aus oder aus einer anderen Anwendung heraus ein Programm starten, welches nicht zugelassen ist, bekommen Sie folgende Fehlermeldung, mit der WinSecure® anzeigt, dass Sie einen nicht erlaubten Vorgang getätigt haben.



Deaktivieren der WinSecure®-Sicherheit:

Sie können jederzeit die Sicherheit von WinSecure® deaktivieren, indem Sie auf das geschlossene Schloss unten rechts in der Taskleiste doppelklicken. Es erscheint der Dialog, um die Sicherheit zu deaktivieren. Verwenden Sie entweder den Benutzer "**WSADMIN**" mit seinem Kennwort oder aber ein Konto und Kennwort eines anderen WinSecure® Administrators. Das kleine Schloss rechts unten öffnet sich dadurch und wird grün. Das bedeutet, dass die Sicherheit nun deaktiviert ist. Jetzt steht Ihnen der Rechner ohne jegliche Einschränkungen wieder zur Verfügung.

Wenn Sie die Option "**Konfigurationsfenster öffnen**" wählen, wird die Sicherheit deaktiviert und das Konfigurationsfenster von WinSecure® wird geöffnet. Sie können das Konfigurationsfenster von WinSecure® auch durch einen Klick mit der linken Maustaste auf das geöffnete Schloss aufrufen.

Solange das Schloss geöffnet ist, funktioniert Ihr Computer wie bisher gewohnt - alle Programme und Einstellungen können genutzt werden.

Ein Zulassen von Hand ist nur dann notwendig, wenn die Standardeinstellungen im Reiter "Dateirechte - Grundeinstellungen für Dateitypen" verschärft wurden. Ansonsten ist die Grundeinstellung so, dass alle installierten Programme ohne Probleme laufen sollten.

Wurden die Grundeinstellungen verschärft, ist folgendes Kapitel zu beachten.

Programme die Sie aus dem Startmenü heraus starten:

Beim Anlegen eines Benutzers haben Sie diejenigen Programme im Startmenü freigegeben, welche vom Benutzer ausgeführt werden sollen. Nicht explizit freigegebene Programme können vom Benutzer nicht genutzt werden.

Teilweise bestehen Programme, z.B. Word, nicht nur aus einer einzigen, sondern aus mehreren ausführbaren Dateien, die sich gegenseitig und automatisch aufrufen. Sehr oft sind beispielsweise Hilfedateien als selbstständige Programme ausgegliedert. Da Sie aber beim Anlegen eines Benutzers lediglich eine Datei pro Startmenüeintrag zugelassen haben, ist es durchaus möglich, dass WinSecure® beim Arbeiten dann Einschränkungen bringt oder aber wichtige Programmteile eine Fehlermeldung verursachen. Dies geschieht genau dann, wenn das freigegebene Programm, z.B. Word,

ein anderes, ausführbares Programm aufrufen will, welches wiederum für sich noch nicht freigegeben wurde. WinSecure® verursacht dann folgende Fehlermeldung:

Zur Beseitigung dieser Situation benutzen Sie bitte den **Scanmodus**. Sie können damit das oder die fehlenden Programme zu den "zugelassenen Programmen" hinzufügen.

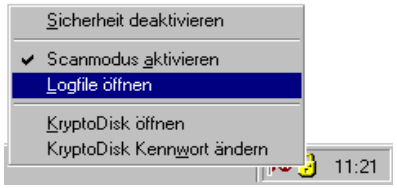
Gehen Sie dabei bitte wie folgt vor:

1. *Klicken Sie mit der Maus ein Mal auf das rote, geschlossene Schloss.*
2. *wählen Sie aus dem Menü den Menüpunkt "**Scanmodus aktivieren**". Sie werden dann nach dem Konto und Kennwort eines Administrators gefragt,*
3. *welches Sie dann in das Textfeld eingeben.*

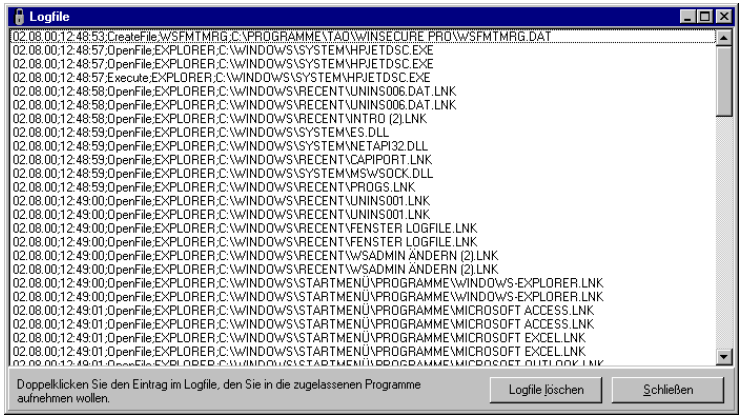
Danach ist der Scanmodus aktiviert. Sie erkennen dies daran, dass das WinSecure®-Schloss in der Taskleiste seine Farbe von rot nach gelb verändert hat.

Bei aktiviertem Scanmodus sind nun alle Einschränkungen, die mit geschlossenem Schloss gelten, aufgehoben. Sie können nun in dieser Phase alle beliebigen Programme starten. Selbst Ihr Startmenü ist wie mit deaktivierter Sicherheit zu erreichen. Versuchen Sie jetzt nochmals alle Programme zu starten, bei denen Sie zuvor eine Einschränkung oder Fehlermeldung bekommen oder eine Fehlfunktion in einem Ihrer Programme festgestellt haben. Alle Programmstarts müssen nun fehlerfrei laufen.

Sind Sie damit fertig, so klicken Sie mit der linken Maustaste auf das gelbe Schloss. Wählen Sie dann den Menüpunkt "**Logfile öffnen**" aus.



Danach zeigt Ihnen WinSecure® alle Aktivitäten, die bei aktivierter Sicherheit abgewiesen worden wären, in einer Liste. Für jede verbotene Aktion wird eine extra Zeile angezeigt. Dies könnte beispielsweise so aussehen:



Alle Zeilen sind nach dem selben Muster aufgebaut. Von links nach rechts, jeweils durch Strichpunkt getrennt, sind dem Logfile folgende Informationen zu entnehmen:

1. *Datum,*
2. *Uhrzeit,*
3. *welche Aktion wurde auf eine entsprechende Datei ausgeführt,*
4. *von welchem Programm wurde eine Aktion auf eine Datei ausgeführt,*
5. *auf welche Datei sollte eine Aktion ausgeführt werden.*

Suchen Sie nun diejenigen Zeileneinträge, welche für eine fehlerfreie Ausführung der entsprechenden Programme gebraucht werden. Meistens gibt Ihnen der Name des Programms, z.B. Word, welches nicht fehlerfrei gestartet ist, den Hinweis auf die noch gesperrten Dateien. Das Wort “Word” ist dann meistens in der entsprechenden Zeile des Logfiles zu finden. Mit einem Doppelklick der linken Maustaste auf die entsprechende Zeile können Sie jetzt den Eintrag und damit die noch gesperrte Datei automatisch zu den “**zugelassenen Dateien**” hinzufügen. Sie geben damit WinSecure® die benötigten, aber vorher noch gesperrten Dateien zur Ausführung frei.

Wenn Sie alle Dateien zugelassen haben, die Sie für die Ausführung des entsprechenden Programms für notwendig halten, schließen Sie das Logfile und deaktivieren Sie den Scanmodus wieder mit einem Klick auf das Schloss und einem weiteren Klick auf “**Scanmodus aktivieren**”. Danach sollte das Schloss wieder seine ursprüngliche rote Farbe bekommen.

Versuchen Sie bitte jetzt nochmals, sämtliche Programme zu starten, welche beim vorherigen Versuch noch Fehlermeldungen verursacht haben. Sollten jetzt immer noch Fehlermeldungen erscheinen, müssen Sie die vorher beschrieben Prozedur mit dem Scanmodus unter Umständen mehrfach wiederholen, damit wirklich alle von den freigegebenen Programmen benötigten Dateien zur Ausführung zugelassen werden. Zur Erleichterung des Vorgangs sollten Sie das Logfile löschen, bevor sie den Scanmodus beenden und wieder neu starten.

!! Wichtig !!

In der Regel sind nur *.exe, *.com, *.bat, -Dateien zuzulassen. Dateien mit der Erweiterung *.lnk kommen durch den Aufruf des Startmenüs und brauchen nicht beachtet zu werden.

Programme die beim Booten des Rechners automatisch gestartet werden:

Wenn Ihr PC bestimmte Programme bereits beim Booten des Rechners startet, kann das vorher beschriebene Problem mit dem oben beschriebenen Weg “Scanmodus” nicht gelöst werden: Das Logfile im “Scanmodus” zeichnet Zugriffe erst nach der Aktivierung des “Scanmodus” auf.

Parallel zum Scanmodus führt WinSecure® allerdings ein zweites Logfile mit, in dem alle abgewiesenen Aktionen dokumentiert werden. In diesem Logfile können Sie auch diejenigen Programme sehen, die beim Starten des Rechners abgewiesen wurden.

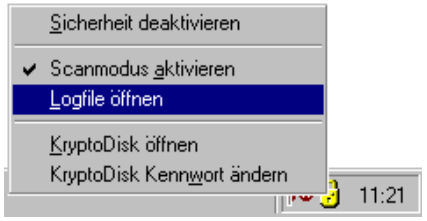
Klicken Sie dazu einmal mit der linken Maustaste auf das rote Schloss und wählen Sie die Option **“Logfile öffnen”**.

Möglicherweise befinden sich sehr viele Einträge in diesem Logfile, so dass es sinnvoll ist, bei einem speziellen Problem zuerst das komplette Logfile zu löschen. Starten Sie nach dem Löschen des Logfiles den Rechner nochmals neu. WinSecure® wird dann beim Booten alle abgewiesenen Aktionen in dieses Logfile schreiben. Nachdem der Rechner vollständig hochgefahren ist, öffnen Sie noch einmal das Logfile. Jetzt sehen Sie im Logfile lediglich diejenigen Einträge, die seit dem letzten Starten des Rechners aufgezeichnet wurden. Durch Doppelklicken mit der Maus auf die einzelnen Zeilen im Logfile können Sie diese dann zu den “zugelassenen Dateien” hinzufügen. Die Zeilen verschwinden dann im Logfile und sind anschließend im Textfeld des Reiters “Dateien zulassen” zu finden. Wenn Sie alle nötigen Dateien zugelassen haben, starten Sie den Rechner bitte nochmals neu. Jetzt sollten keine Fehlermeldungen mehr erscheinen und alle Programme ordnungsgemäß autogestartet werden.

Starten des Computers im Scanmode:

In sehr seltenen Fällen kann es vorkommen, dass ein PC nach der automatischen Aktivierung von WinSecure® komplett seinen Dienst verweigert. Schalten Sie in diesem Fall den PC kurz aus und dann wieder ein. Noch bevor die Anmeldemaske erscheint werden Sie gefragt, ob WinSecure® bei diesem Start im Scanmode gestartet werden soll. Wenn Sie diese Frage mit “**Ja**” beantworten und sich durch die Eingabe eines gültigen Accounts der Gruppe WSADMINS autorisieren, wird WinSecure® den

PC im Scanmode starten und gesperrte Dateien lediglich protokollieren. Sobald der PC komplett gestartet ist, klicken Sie mit der rechten Maustaste auf das gelbe Schloss und fragen wie bereits beschrieben das Logfile ab.



Aus der angezeigten Liste doppelklicken Sie auf die entsprechenden Einträge um Sie in Winsecure® zu den zugelassenen Dateien hinzuzufügen.

3.2.7. Autostarten von Programmen

Prinzipiell können unter WinSecure® alle Programme automatisch gestartet werden. Es spielt dabei keine Rolle, ob Sie Programme aus der Registry heraus starten, aus dem Autostartmenü oder aus der win.ini.

Wenn Sie die Grundeinstellungen im Reiter “Dateirechte - Grundeinstellungen für Dateitypen” verschärft haben, ist folgender Abschnitt zusätzlich zu beachten:

Nachdem Sie WinSecure® installiert haben, werden Sie feststellen, dass nahezu keines Ihrer automatisch gestarteten Programme laufen wird. Dies liegt daran, dass Sie auch diese Programme zuerst freigeben müssen.

Gehen Sie dazu bitte wie folgt vor:

1. *Fahren Sie den Rechner hoch und öffnen Sie die WinSecure® Administration.*
2. *Dort gehen Sie zum Reiter “Dateien zulassen”.*
3. *Öffnen Sie das Logfile, indem Sie auf den Button “Logfile öffnen” klicken. Sie bekommen dann das Logfile zu sehen. Im Logfile werden alle Aktivitäten protokolliert, die WinSecure® abgewiesen hat. Es stehen in dem Logfile also auch diejenigen Dateien, die zum Autostart der ausgewählten Programme benötigt werden.*
4. *Suchen Sie jetzt die entsprechenden Einträge heraus und klicken sie mit Doppelklick der linken Maustaste auf die entsprechenden Zeilen. Damit wird die angeklickte Zeile aus dem Logfile verschwinden und wird im Reiter “Da teien zulassen” in dem Textfeld erscheinen.*

Sollte beim erstmaligen Öffnen das Logfile sehr groß und unübersichtlich sein, empfiehlt es sich, zuerst das Logfile zu löschen und den Rechner nochmals neu zu starten und nach dem Neustart das Logfile nochmals anzusehen. Dies hat den Vorteil, dass jetzt nur diejenigen Dateien angezeigt werden, die während des Startvorganges abgewiesen wurden.

Wenn Sie alle Dateien auf diese Art und Weise hinzugefügt haben, sollten die Programme auch mit aktivierter Sicherheit gestartet werden können. Bei Bedarf müssen Sie den gerade beschriebenen Vorgang mehrfach wiederholen.

4. Die WinSecure® Administration

Die WinSecure® Administration bietet Ihnen ergänzend zum Benutzerassistent noch weitere Möglichkeiten der Administration von WinSecure® bzw. WinSecure® Benutzern. Öffnen Sie bitte die Administration von WinSecure® bei deaktivierter Sicherheit entweder über das Startmenü oder durch einen Klick mit der linken oder rechten Maustaste auf das WinSecure®-Schloß in der Taskleiste. Das Administrationsmenü stellt ihnen verschiedene Reiter zur Administration zur Verfügung.

Ist WinSecure® nicht gestartet so müssen Sie sich zuerst als Administrator an WinSecure® anmelden um die Administration öffnen zu können.

4.1. Der Reiter Information

Im Reiter “**Information**” sehen Sie, ob WinSecure® bereits lizenziert ist. Unten rechts sehen Sie, dass bereits eine Lizenz für Klaus Mustermann vorliegt. Sollte unten rechts “unlizenziert” stehen, können Sie entweder eine Lizenz von Ihrem WinSecure® Server beziehen oder von der Lizenzdiskette, die mit der Software mitgeliefert wurde.

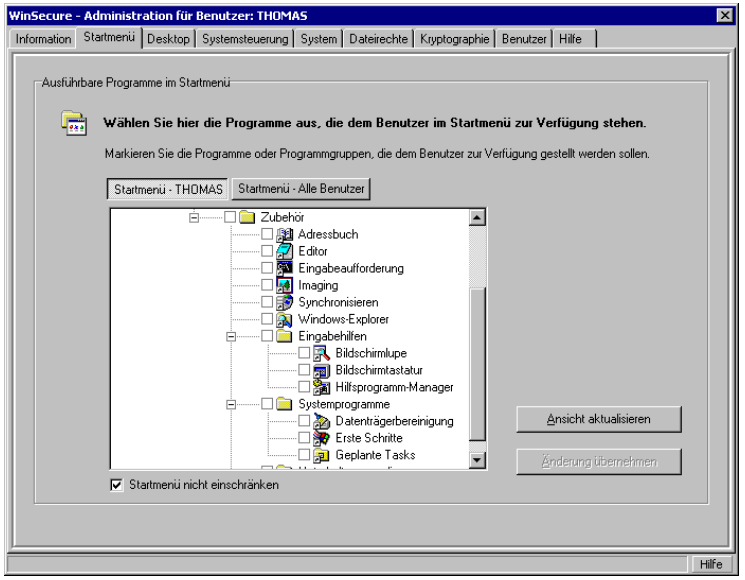
Mit dem Button “Lizenz zurückschreiben” können Sie eine Lizenz anfordern, bzw. wenn Sie schon eine Lizenz haben, können Sie diese wieder auf den Server bzw. auf die Diskette zurückschreiben. Wenn im Reiter “Benutzer” eine gültige IP-Adresse des WinSecure® Servers vorliegt, wird stets versucht, die Lizenz vom Server zu holen, bzw. auf diesen die Lizenz wieder zurückzuschreiben. Wenn Sie dort 127.0.0.1 stehen haben, betrachtet WinSecure® die Installation als lokal und fordert Sie auf, die Lizenz-Diskette mit der dieser Client lizensiert wurde, einzulegen. Beachten Sie bitte beim Zurückschreiben einer Lizenz, dass dies nur auf genau die Diskette erfolgen kann, von der aus dieser PC lizenziert wurde.

4.2. Der Reiter Startmenü

Sobald Sie mit der Maus den Reiter “**Startmenü**” auswählen, wird automatisch das Startmenü ausgelesen. Dies kann bei umfangreichen Startmenüs etwas Zeit in Anspruch nehmen. Alle Programme, die für den aktuell angemeldeten Benutzer bereits zugelassenen wurden, sind mit einem Häkchen markiert. Sie können nun mit Hilfe der Maus und den Scrollbars das Startmenü der installierten Programme ansehen und durch ein Häkchen die jeweiligen Programme für den in Bearbeitung befindlichen Benutzer (jetzt gerade THOMAS) auswählen und damit freigeben. Die Programme, die Sie hier auswählen, werden für den aktuellen Benutzer im Startmenü angezeigt. Dabei ist es auch möglich, die vorhandenen Baumstrukturen zu nutzen. Alle Programme die Sie hier nicht ausdrücklich angehakt haben, werden später im Startmenü nicht mehr zu sehen sein und können auch nicht aus anderen Applikationen heraus gestartet werden. Auch mit dem Windows-Explorer ist es dem nicht Anwender möglich, Programme zu starten, wenn Sie nicht vorher im Reiter “Startmenü” explizit freigegeben wurden.

Unter Windows NT, Windows 2000 und Windows XP verfügt jeder Benutzer über ein geteiltes Startmenü. Sowohl sein persönliches Startmenü als auch das Startmenü für alle Benutzer werden dabei zu einer Anzeige addiert. WinSecure® bietet Ihnen die Möglichkeit, beide Menüs entsprechend zu kontrollieren.

Mit der angehakten Checkbox “Startmenü nicht einschränken” kann veranlasst werden, dass das komplette Startmenü trotz aktivierter Sicherheit sichtbar ist.



Mit dem Button “**Änderungen übernehmen**” können Sie die geänderten Einstellungen speichern.

Mit dem Button “**Ansicht aktualisieren**” wird die derzeit gespeicherte Einstellung für diesen Benutzer geladen und angezeigt.

Beachten Sie bitte hierbei, dass Sie eventuell noch Unterprogramme zulassen müssen wenn Sie die Sicherheitseinstellungen verschärft haben. Unterprogramme sind in diesem Zusammenhang ausführbare Programmteile, die von einem Ihrer Programme im Startmenü aufgerufen werden. Oftmals ist die Hilfedatei eines Programms ein selbständiges, ausführbares Unterprogramm. Dieses müssen Sie im Reiter “Zugelassene Dateien” manuell zulassen oder durch Verwendung des Scanmodes im Reiter “Dateien zulassen” eintragen. Falls durch WinSecure® eventuelle Einschränkungen oder Fehlermeldungen erscheinen sollten, empfehlen wir Ihnen, nach der Konfiguration des jeweiligen Benutzers alle freigegebenen Programme zu testen und dabei den Scanmodus zu aktivieren. Näheres über diese Funktion lesen Sie bitte in dem speziellen Kapitel über den Scanmodus.

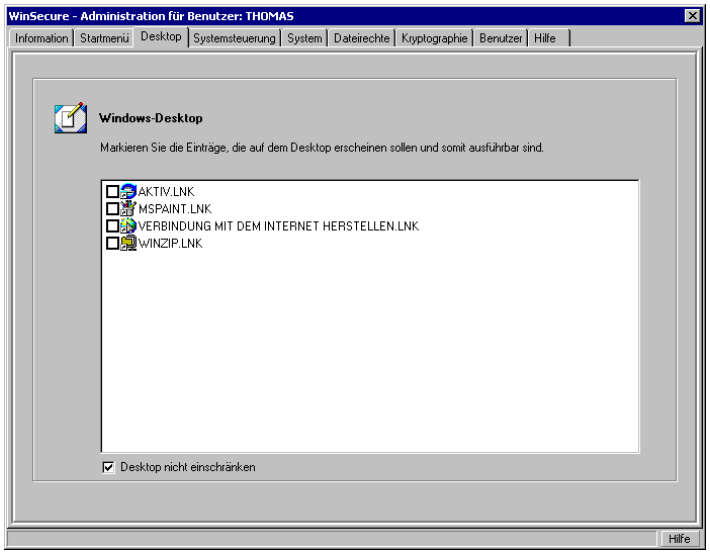
4.3. Der Reiter Desktop

Im Reiter “**Desktop**” können Sie für den gerade in Bearbeitung befindlichen Benutzer die Desktop Icons definieren. Für jeden Benutzer kann eine eigene Einstellung vorgenommen werden. Beachten Sie bitte, dass diese Einstellungen nur dann wirksam sind, wenn Sie im Reiter “**System**” ***nicht*** die Checkbox “**Desktop Icons verstekken**” angehakt haben.

Mit der Checkbox “Desktop nicht einschränken” können sie veranlassen, dass alle Dateien auf dem Desktop sichtbar (manche allerdings nicht ausführbar) sind.

!! Achtung !!

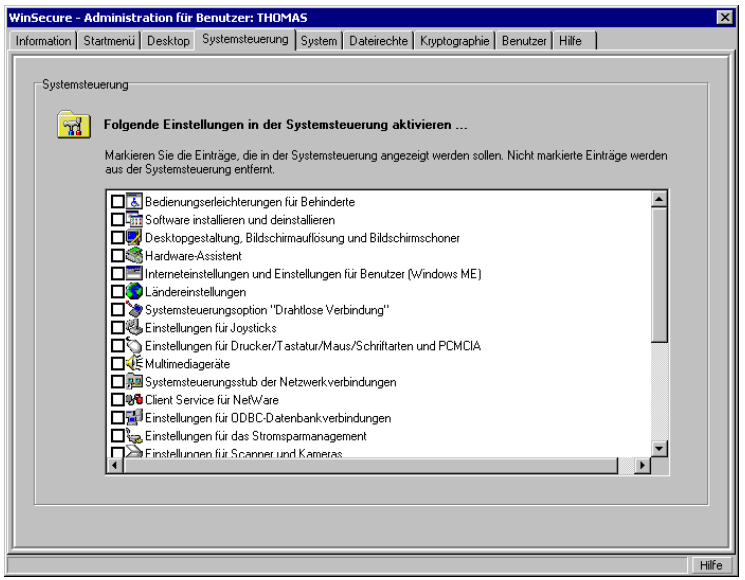
Die Icons im Desktop “Alle Benutzer” werden hier nicht angezeigt können dementsprechend nicht augeblendet werden.



4.4. Der Reiter Systemsteuerung

In dem Reiter “**Systemsteuerung**” können Sie diejenigen Einträge administrieren, die unter Start/Einstellungen/Systemsteuerung zu erreichen sind.

Der voreingestellte Zustand ist, dass dem Benutzer **keine** Einstellungsmöglichkeiten erlaubt sind. Da der Benutzer nur in seltenen Fällen individuelle Einstellungen braucht, empfehlen wir, im Reiter “**Systemsteuerung**” so wenig wie möglich Einstellungsmöglichkeiten freizugeben.



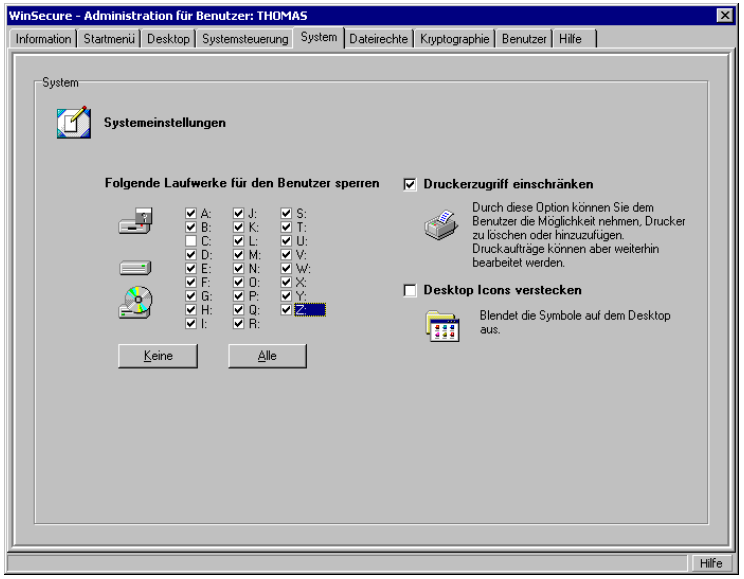
4.5. Der Reiter System

Folgende Laufwerke für den Benutzer sperren

Jedes Laufwerk, welches in dem nebenstehenden Kästchen angehakt ist, ist damit für den jeweiligen Benutzer komplett gesperrt und somit nicht zugreifbar. Der Sperrschutz von WinSecure® basiert nicht auf Windows-Bordmitteln, sondern geht weit über diese hinaus. WinSecure® arbeitet in dieser Funktion mit einem von Datapol entwickelten und patentierten Filetreiber zum Schutz von Laufwerken, Verzeichnissen und Dateien.

Eine Ausnahme bildet das Systemlaufwerk, meistens ist dies das Laufwerk “C”. Auf dem Systemlaufwerk ist das Betriebssystem installiert. Das Betriebssystem muss wiederum laufend bestimmte Dateien lesen und schreiben. Eine komplette Sperrung dieses Laufwerkes würde zu Problemen bzw. zu einem Systemabsturz führen. Dementsprechend kann dieses Laufwerk in diesem Reiter nicht komplett gesperrt werden. Wenn Sie daher die Sperre für das Systemlaufwerk aktivieren, wird dieses Laufwerk nicht gesperrt, sondern lediglich versteckt.

Wie Sie einzelne Verzeichnisse und Dateien auf dem Systemlaufwerk sperren können lesen Sie bitte im Kapitel “Der Reiter Dateirechte - Spezielle Dateirechte”. In der WinSecure® PROFESSIONAL Edition sind bestimmte Verzeichnisse und Dateien bereits mit sinnvollen Dateiattributen versehen. Damit ist gewährleistet, dass das Betriebssystem nicht beschädigt werden kann.



Druckerzugriff einschränken

Auch wenn Sie den Druckerzugriff für die Benutzer über diese Funktion einschränken, können alle eingerichteten Drucker vom Benutzer genutzt werden. Dem Benutzer ist es aber nicht möglich, einen neuen Drucker hinzuzufügen oder auch bestehende Drucker zu löschen. Sie können damit sicherstellen, dass die Benutzer nur auf definierten Druckern ausdrucken können. Die Konfiguration der Druckeroptionen (Schachtwahl, Wahl der Auflösung...) ist dem Benutzer auch bei aktiviertem Schutz möglich.

Desktop Icons verstecken

Damit ist beim Aktivwerden der Sicherheit der Desktop komplett leer, der Benutzer sieht keine Icons mehr auf seinem Bildschirm. Der Benutzer kann dadurch Programme nur noch über das Startmenü starten. Im Reiter “**Desktop**” können Sie für den gerade in Bearbeitung befindlichen Benutzer alternativ einzelne Desktopsymbole speziell sichtbar und unsichtbar machen.

MS-DOS Modus sperren

Diese Einstellungsmöglichkeit wird unter Windows NT, Windows 2000 und Windows XP nicht angezeigt!

Hiermit können Sie verhindern, dass der Benutzer beim Herunterfahren des Rechners in den DOS-Modus gelangen kann.

!! Achtung !!

Haben Sie zum Beispiel Microsoft Word auf der Festplatte D:\ installiert und dieses Laufwerk gesperrt, Word jedoch im Startmenü zugelassen, so werden Sie beim Start von Word viele Fehlermeldungen erhalten, da z.B. die Normal.dot oder auch die Programmerweiterungen von Word nicht mehr verfügbar sind!

Unter Windows NT, Windows 2000 und Windows XP können alle Wechseldatenträger (Floppy, CD-ROM, ZIP...) derzeit nur hier gesperrt werden. Wenn diese Laufwerke nicht komplett gesperrt sind können beliebige Programme von ihnen gestartet werden.

4.6. Der Reiter Dateirechte - Grundeinstellungen für Dateitypen

In diesem Reiter können Sie die grundsätzlichen Sicherheitseinstellungen für Dateitypen einstellen. Es können vier Schutzstufen eingestellt werden:

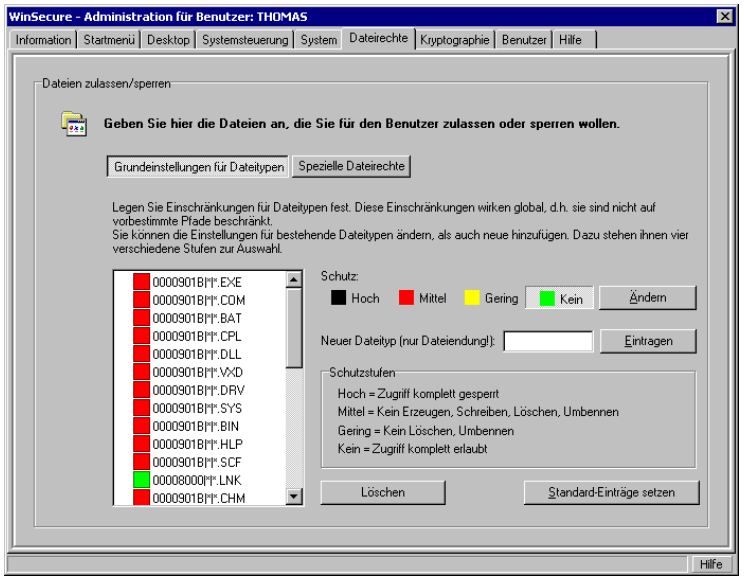
1. *Hoch*
2. *Mittel*
3. *Gering*
4. *Kein*

Aufgrund der links angezeigten Farben sieht man sofort, welche Dateirechte für den entsprechenden Dateityp gesetzt sind.

In der bei der Installation angelegten Liste sind die häufigsten Dateitypen aufgeführt, wenn allerdings noch ein Dateityp fehlen sollte, kann dieser mit dem Button “Eintragen” und dem Eingabefeld “Neuer Dateityp” hinzugefügt werden.

Welche Sicherheitseinstellungen für die einzelnen Schutzstufen gewählt sind, ist im Kapitel über die Speziellen Dateirechte erläutert.

Mit dem Button “Standardeinträge setzen” können die im Reiter “Grundeinstellungen” und “Spezielle Dateirechte” getroffenen Einstellungen wieder zurückgesetzt werden. Dieser Button stellt allerdings lediglich die voreingestellten Regeln wieder her. Regeln die über dies hinaus getroffen wurden, werden nicht gelöscht.



4.7. Der Reiter Dateirechte - Spezielle Dateirechte

!! ACHTUNG !!

Die hier vorgenommenen Einstellungen können Ihr System zum Absturz bringen! Testen Sie bitte die hier vorgenommenen Einstellungen vor einem Rollout sehr gründlich. Machen Sie sich unbedingt mit den Regeln nach denen WinSecure® arbeitet vertraut.

Lesen Sie auch das Beispiel in diesem Abschnitt.

Mit den nachfolgenden Punkten sollten Sie auf jeden Fall betraut sein:

1. Die Rechtevergabe und Sortieregeln von WinSecure®

2. Die Rechte auf Dateien und Verzeichnisse, die Ihre Anwendungen benötigen um fehlerfrei zu arbeiten.

3. Der Umgang mit dem Scanmodus und dem Logfile von WinSecure®.

Der Scanmodus und das Logfile stehen Ihnen immer hilfreich zur Seite um zu erfahren, warum etwas nicht wie gewünscht funktioniert.

Einträge in “**gesperrten Dateien**” können nur manuell vorgenommen werden.

Zur manuellen Eingabe müssen Sie sowohl den Pfad als auch die Maske der zur behandelnden Dateien oder Verzeichnisse in die Eingabefelder eintragen.

Besondere Masken sind hierbei:

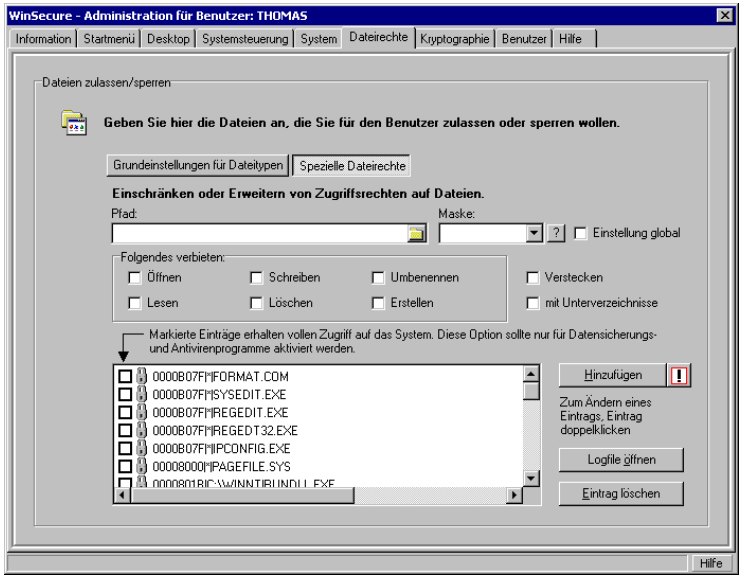
“.” - bezieht sich auf das Verzeichnis (ohne Inhalt)

“*.*” bezieht sich auf alle Dateien im angegebene Pfad (ohne Unterverzeichnisse)

“*.xxx” bezieht sich auf alle Dateien mit der Erweiterung xxx im angegebene Pfad (ohne Unterverzeichnisse)

Der einzige besondere Pfad

ist über die Checkbox “Einstellungen global” erreichbar. Mit dieser Option werden alle Dateien der angegebenen Maske mit den entsprechenden Rechten versehen.



Die auswählbaren Rechte im Einzelnen:

- *Öffnen: Verhindert das Öffnen einer Datei. Das Öffnen einer Datei entspricht der Entnahme des Inhalts.*
- *Lesen: Verhindert das Lesen einer Datei. Das Lesen einer Datei entspricht der kompletten Übertragung seines Inhalts*
- *Schreiben: Verhindert das Schreiben von Änderungen an den angegebenen Dateien.*

- *Löschen: Verhindert das Löschen von Dateien.*
- *Umbenennen: Verhindert es, der Datei einen anderen Namen zu geben.*
- *Verstecken: Verbirgt die Datei vor dem Anwender (auch wenn im Explorer versteckte Dateien anzeigen ausgewählt ist)*
- *Erstellen: Verhindert das Erzeugen einer neuen Datei*
- *mit Unterverzeichnissen: Die Einstellung bezieht sich auch auf alle unterge ordneten Verzeichnisse*

Jede Datei auf einem Datenträger kann man sich vorstellen wie eine Kiste, die eine Aufschrift enthält. Verschiedene Dinge, die man mit dieser Kiste anfangen kann, entsprechen den Fileattributen von WinSecure:

1. *Die Aufschrift auf der Kiste entspricht dem Dateinamen.*
2. *Das Deckelschloss der Kiste entspricht dem Attribut „OpFi". Für alle Datei operationen bei denen man an den Inhalt der Datei herankommen muss, muss auch „OpFi" freigegeben sein.*
3. *Der Inhalt der Kiste wird mit dem Attribut „RdFi" ausgelesen. Dabei ist es nicht von Bedeutung, ob der Inhalt der Datei eine Textdatei ist oder eine ausführbare Binärdatei. Bevor man den Inhalt der Datei auslesen kann, muss diese zuerst mit „OpFi" geöffnet werden.*
4. *Das Attribut „WrFi" entspricht dem erneuten Befüllen der Datei. Um in eine Datei schreiben zu können, müssen auch die Attribute „OpFi" und „RdFi" erlaubt sein.*
5. *Das Attribut „DelFi" verhindert das komplette Löschen der Kiste. Wenn die ses Attribut gesetzt ist, darf die Datei auch nicht umbenannt werden, da dies einer Löschung der Datei gleichkommen würde.*
6. *Das Attribut „RenFi" verhindert, dass die Kiste einen neuen Namen bekommt. Dies funktioniert allerdings erst, wenn auch das Attribut „DelFi" zugelassen ist.*
7. *Mit dem Attribut „MkFi" kann man verhindern, dass eine Kiste mit der angege benen Aufschrift erstellt werden kann. Die gilt auch für das Erstellen durch Umbenennen.*
8. *Mit dem Attribut „Hide" kann man die vorhandene Kiste unsichtbar machen.*
9. *Mit dem Attribut „SubFo" kann man auch die entsprechenden Kisten in den darunter liegenden Verzeichnissen ansprechen.*

Sie können einen Eintrag bearbeiten, indem Sie ihn durch einen Doppelklick in die Bearbeitungszeile holen. Nachdem Sie die Korrekturen an Pfad, Maske oder Rechten vorgenommen haben, können Sie den geänderten Eintrag durch "**Hinzufügen**" wieder in die Liste übertragen.

Links von jeder Zeile ist jeweils eine Checkbox für jeden Eintrag vorgesehen, mit der man einem Programm Vollzugriff auf die Datenträger gewähren kann. Ein Vollzugriff ist z.B. sinnvoll für das Ausführen von bei Backup-Programmen oder Virenscannern. WinSecure® ist so eingestellt, dass der Benutzer keinen Zugriff auf bestimmte Dateien und Ordner hat. Mit dieser Checkbox kann man diesen Schutz bzw. Sperrung für alle hier explizit freigegebenen Programme ausschalten . Wenn Sie also für Ihr Backup-Programm kein Häkchen setzen, hat dieses keine Möglichkeit, geschützte Ordner zu sichern.

!! Achtung !!

DOS und 16Bit Windowsprogrammen werden keine Sonderrechte über diese Checkbox eingeräumt!

Alle Programme die über Vollzugriff verfügen sind vor allem dann gefährlich, wenn Sie über den Standard Datei-Öffnen Dialog verfügen.

4.8. Der Reiter Kryptographie

Für sicherheitsrelevante Daten bietet WinSecure® optional die Möglichkeit an, benutzerspezifische Daten auf einem speziellen Datenträger **verschlüsselt** abzulegen. Dabei steht für die Benutzer ein virtuelles Laufwerk zur Verfügung, auf dem die dort gespeicherten Daten dann verschlüsselt abgelegt werden können.

WinSecure® bietet dem Benutzer drei verschiedene Verschlüsselungsverfahren an:

- *Zum Ersten eine 3DES-Verschlüsselung mit einer Schlüssellänge von 168 Bit,*
- *zum Zweiten WSummer mit einer Schlüssellänge von 128 Bit und*
- *schließlich den Verschlüsselungsalgorithmus Blowfish mit einer Schlüssel länge von 245 Bit.*

Sie müssen sich aber nicht um die Verschlüsselung an sich kümmern. Die Verschlüsselung läuft für den Anwender unsichtbar im Hintergrund ab. Das Kryptolaufwerk wird nach der Eingabe eines Passwortes geöffnet. Während der Sitzung können Daten auf das verschlüsselte Laufwerk abgelegt und bearbeitet werden. Der Datentresor kann jederzeit geschlossen werden. Spätestens nach dem Abmelden wird der Datentresor geschlossen und kann außer vom Benutzer von niemand anderem mehr gelesen werden. Dies gilt auch für den Administrator.

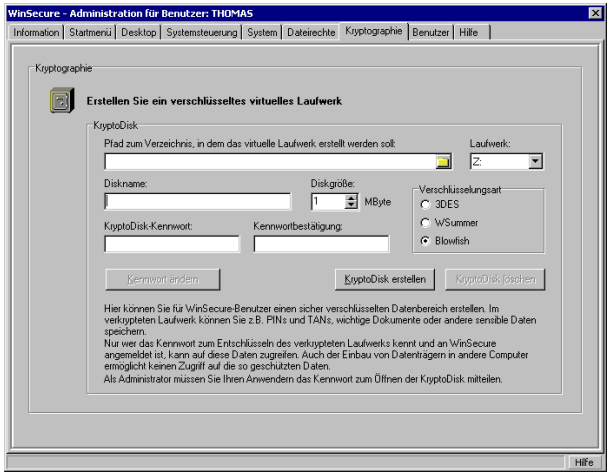
Wenn Sie eine Kryptodisk anlegen wollen, öffnen Sie den Reiter “**Kryptographie**”. Als erstes müssen Sie nun den Speicherort der Kryptodisk angeben. Dies machen Sie, indem Sie auf den Ordnerbutton klicken. Um Tipp und Schreibfehler zu vermeiden ist es nicht vorgesehen, in die Pfadzeile manuell etwas einzutragen. Wählen Sie dann im sich öffnenden Explorerfenster den Speicherort ihrer Kryptodisk. In unserem Beispiel wäre dies C:\.

Geben Sie in dem Feld “**Diskname**” Ihrer Kryptodisk einen Namen. Diesen können Sie beliebig wählen. Unter dem hier angegebenen Namen wird Ihre Kryptodisk später im Windows-Explorer zu finden sein.

Weisen Sie der Kryptodisk eine “**Diskgröße**” zu. In unserem Beispiel beträgt die Größe 500 MByte. Sie müssen sich vorher überlegen, wie groß die Diskgröße sein soll***, da Sie die Größe der Kryptodisk später nicht mehr ändern können***. Beachten Sie dabei auch, dass beim Anlegen der Kryptodisk der angegebene Speicherplatz sofort in Anspruch genommen wird und anderweitig nicht mehr verwendet werden kann. Dies gilt auch dann, wenn auf dem Kryptolaufwerk noch keine Daten gespeichert sind.

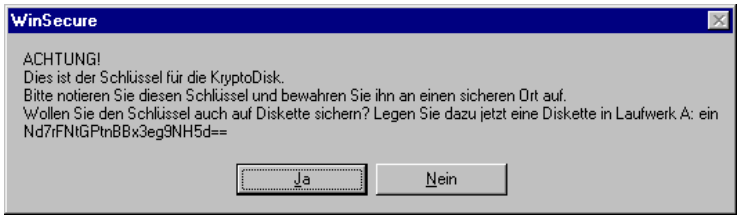
Wählen Sie dann ein “**Passwort**”, um Ihre Kryptodisk später wieder öffnen zu können und entscheiden Sie sich für einen der 3 Verschlüsselungsalgorithmen. Die verschiedenen Verschlüsselungsarten unterscheiden sich etwas voneinander. Alle drei sind sehr sicher und haben sich als allgemeiner Standard etabliert. Wenn Sie bisher allerdings noch keine Erfahrung mit Verschlüsselungsalgorithmen hatten und daher auch die Unterschiede nicht kennen, empfehlen wir Ihnen den **Blowfish-Algorithmus** zu wählen.

Mit dem Drücken des Buttons “**KryptoDisk erstellen**” wird Ihr neues Laufwerk erstellt.

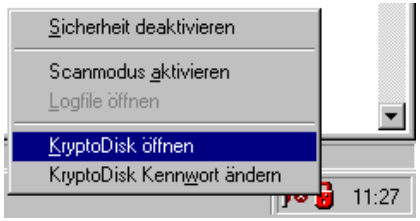


Nachdem WinSecure® Ihr Kryptolaufwerk angelegt hat, wird Ihnen noch der Schlüssel mitgeteilt, mit dem WinSecure® Ihre Daten verschlüsseln wird. Dieser Schlüssel benötigen Sie ggf. für den Zugriff auf Ihre Daten im Kryptolaufwerk.

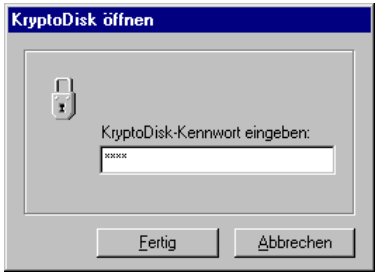
Wichtig: ***Bitte notieren Sie sich den Schlüssel*** *und* ***speichern ihn zusätzlich noch auf einer Diskette. Achten Sie bitte unbedingt dabei darauf, dass Sie diesen Schlüssel an einem sicheren Ort aufbewahren. Zur täglichen Arbeit mit WinSecure® brauchen Sie allerdings diesen Schlüssel nicht.***



Um Ihr neues Laufwerk zu testen, aktivieren Sie die Sicherheit mit einem Klick der rechten Maustaste auf das geöffnete Schloss und klicken dann auf “**Sicherheit aktivieren**”. Danach klicken Sie nochmals mit der linken Maustaste auf das nun geschlossene Schloss und bekommen dann folgende Auswahl zu sehen:

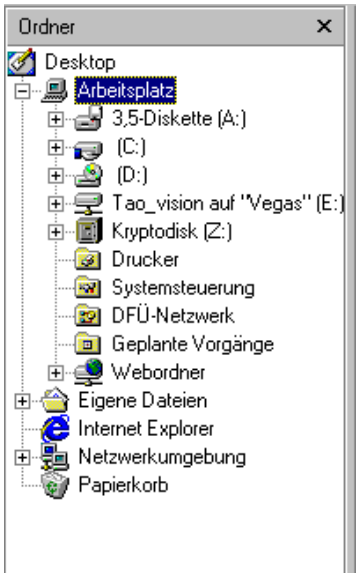


Klicken Sie auf “**KryptoDisk öffnen**”. Sie werden aufgefordert, das Passwort für die Kryptodisk einzugeben:



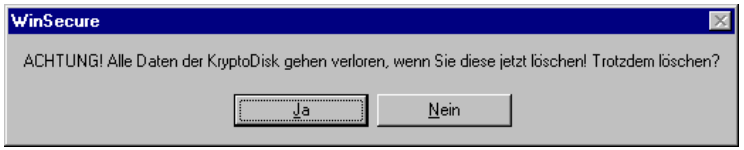
Wenn Sie den Windows-Explorer zugelassen haben, können Sie nun das neu angelegte Laufwerk betrachten. In unserem Fall trägt es den Namen “Kryptodisk” und hat den Laufwerksbuchstaben Z erhalten.

Sie können nun das Kryptolaufwerk wie Ihr gewöhnliches Laufwerk “C” oder ein Netzlaufwerk verwenden.



Es ist auch möglich, das Kryptolaufwerk zu löschen. Dies kann dann notwendig werden, wenn Sie ein Laufwerk angelegt haben, sich aber dann doch entschließen, Ihre Daten nicht verschlüsselt zu speichern. Außerdem kann auch der Fall auftreten, dass Sie schon längere Zeit mit dem Kryptolaufwerk arbeiten und das Speichervolumen des Kryptolaufwerkes zu klein wird. In diesem Fall sollten Sie sämtliche Daten an einen sicheren Ort kopieren, dann das vorhandene Kryptolaufwerk löschen, ein größeres Kryptolaufwerk anlegen und danach die Daten wieder zurückkopieren.

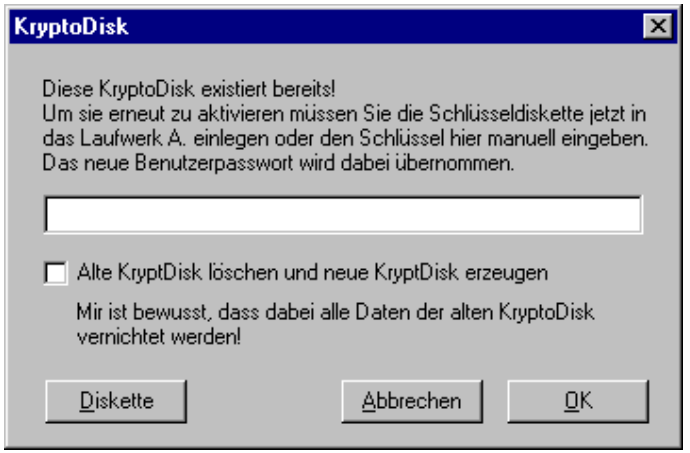
Zum Löschen des Kryptolaufwerks deaktivieren Sie die Sicherheit und öffnen Sie den Reiter “Kryptographie”. Danach drücken Sie den Button “Kryptodisk löschen” und klicken Sie im folgenden Fenster auf “Ja”. Damit ist Ihr Kryptolaufwerk und damit auch sämtliche darin beinhaltete Daten gelöscht und der vom Kryptolaufwerk beanspruchte Speicherplatz steht wieder zur Verfügung.



Wenn Sie den Vorgaben bei der Erstellung des Datentresors folgen, befinden sich Ihre verschlüsselten Daten in der Datei “**benutzername.cry**. Das Wort “**benutzername**” steht dabei für den gerade angemeldeten Benutzer. Wenn beispielsweise der Benutzer “**Thomas**” angemeldet ist, würde die Kryptodatei “**Thomas.cry**” heißen. Es kann für jeden Benutzer also **genau eine** Kryptodisk angelegt werden. Die Kryptodatei befindet sich in dem Pfad, den Sie beim Anlegen der Kryptodisk angegeben haben. Bei Defekt ihrer Festplatte oder bei versehentlichem Löschen des Kryptofiles, können Sie durch manuelle Eingabe des “langen” Schlüssels, den Sie sich aufgeschrieben haben oder bei der Erstellung auf Diskette gespeichert haben Ihr Kryptolaufwerk von Ihrem Backup wiederherstellen.

Wenn Sie also auf Grund eines Festplattenfehlers den Rechner neu aufsetzen müssen, melden Sie sich nach der erneuten Installation von WinSecure® als derjenige Benutzer an, unter dem Sie die Kryptodisk erstellt haben und deaktivieren Sie die Sicherheit. Im Reiter “**Kryptographie**” sind jetzt keine Eintragungen mehr vorhanden. Falls noch Eintragungen vorhanden sind, sollten Sie **VOR** der Wiederherstellung der Datei “**benutzername.cry**” die bestehende Kryptodisk löschen.

Nach der Rücksicherung der Datei “**benutzername.cry**” von ihrem Backup-System (in unserem Fall nach C:\) verhalten Sie sich so, als wollten Sie eine neue Kryptodisk in exakt demselben Pfad erstellen. WinSecure® zeigt dann mit folgender Meldung, dass in diesem Pfad bereits ein Kryptolaufwerk besteht:

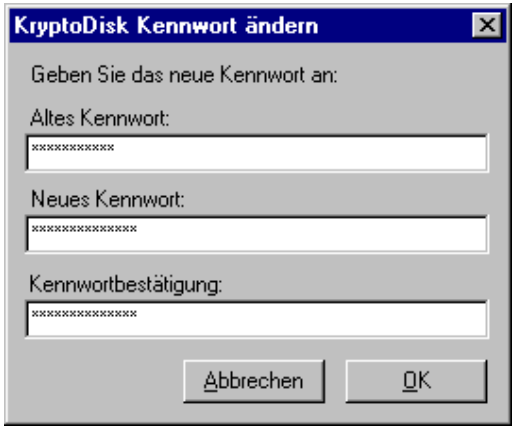


Jetzt können Sie die beim Anlegen des Kryptolaufwerks angelegte Diskette einlegen und auf “Diskette” klicken oder aber den Zifferncode von Hand in das Eingabefeld eintragen. Nachdem der Zifferncode des “langen” Schlüssels komplett im Eingabefeld steht, können Sie auf “OK” klicken. WinSecure® meldet Ihnen dann, dass das bereits vorhandene Laufwerk erfolgreich wiederhergestellt wurde.

Sie können dieses Verfahren auch verwenden, wenn Sie Kryptolaufwerke mit anderen Benutzern austauschen wollen. So ist es z.B. möglich, die Datei "**benutzername.cry**" auf eine CD zu brennen und zu versenden. Wenn Ihr Partner den Masterschlüssel zum Kryptolaufwerk hat, wird er es öffnen können. Dazu muss Ihr Partner allerdings auch an einem abgesicherten WinSecure PC arbeiten.

Ändern des Benutzerkennworts für einen Datentresor

Grundsätzlich kann es bei der Verwendung eines Datentresors vorkommen, dass Ihnen jemand bei der Eingabe des Kennworts über die Schulter geschaut hat und das Kennwort damit nutzlos ist. WinSecure® bietet Ihnen deshalb die Möglichkeit, das "kurze" Kennwort für den Datentresor jederzeit und einfach zu ändern.



Nach Änderung des Kennwortes können Sie den Datentresor nur noch mit dem neuen Kennwort öffnen.

Wichtig:

Der Masterschlüssel für den Datentresor bleibt jedoch unverändert erhalten und verliert durch die Änderung des Kennwortes seine Gültigkeit nicht.

4.9. Der Reiter Benutzer

Mit dem Reiter "**Benutzer**" können Sie Ihre WinSecure®-Benutzer verwalten. In der blau hinterlegten Kopfzeile wird stets der gerade in Arbeit befindliche Benutzer angezeigt. In unserem Fall ist das der Benutzer "THOMAS". Alle Einstellungen, die Sie jetzt in den anderen Reitern vornehmen, gelten für diesen Benutzer.

IP-Adresse des Servers festlegen

Wenn Sie wie im unteren Bild den Button "**Benutzer hinzufügen/Server einrichten**" gedrückt haben, können Sie im oberen Bereich die WinSecure® Benutzer definieren und im unteren Bereich die IP-Adresse des WinSecure® Servers festlegen. Stellen Sie sicher, dass Sie auf einem anderen Rechner einen WinSecure® Server installiert haben und dieser dort auch gestartet ist. Stellen Sie auch sicher, dass dessen IP-Adresse sich nicht ändert.

Benutzen Sie daher keinen DHCP-Server für die Vergabe der IP-Adresse des WinSecure®-Servers.

Wenn Sie den WinSecure® Server gestartet haben und die IP-Adresse im unteren Feld eingetragen ist, testen Sie die Verbindung indem Sie auf "Test" klicken. Es wird dann eine kurze Testverbindung zum Server hergestellt und WinSecure® sagt Ihnen, ob ein Server gefunden wurde.

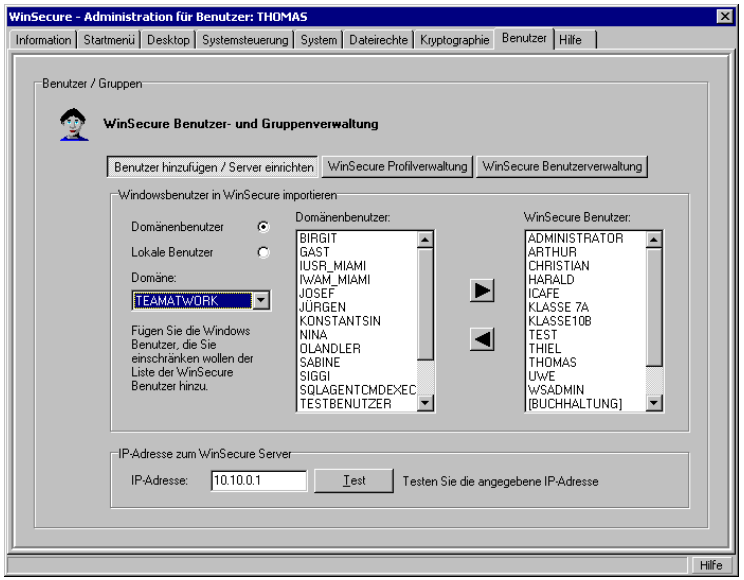
Wenn Sie keinen WinSecure® Server verwenden, müssen Sie den integrierten WinSecure® Server verwenden. Dieser ist bei allen WinSecure® Clients eingebaut. Bitte tragen Sie in diesem Fall in dem Feld Server IP-Adresse die nachfolgende IP Adresse "**127.0.0.1**" ein. Dies beschreibt die Loopbackadresse und damit denselben Rechner.

Benutzer hinzufügen / Server einrichten

Im oberen Bereich können Sie bereits existierende Benutzer als WinSecure® Benutzer definieren. Je nachdem, ob Sie die Checkbox "**Domänenbenutzer**" oder "**Lokale Benutzer**" aktiviert haben, werden Ihnen im linken Anzeigefeld die Domänenbenutzer oder die Lokalen Benutzer angezeigt. Wenn Sie die Domänenbenutzer sehen wollen müssen Sie in der Pop-Up Box "Domäne" die entsprechende Domäne einstellen.

Wählen Sie nun mit Hilfe der Maus und der Scrollbar im linken Anzeigefeld den- oder diejenigen Benutzer aus, für die Sie eine WinSecure® Anmeldung benötigen. Markieren Sie diesen mit der Maus so dass er blau hinterlegt wird. Klicken Sie dann auf den Button mit dem Rechtspfeil, um den markierten Benutzer in das rechte Anzeigefeld "**WinSecure® Benutzer**" zu kopieren. Wie Sie sehen, sind die unteren vier Benutzer im rechten Anzeigefeld in rechteckigen Klammern. Damit werden Benutzergruppen dargestellt. Falls Sie mehrere Benutzer mit genau identischen Einstellungen haben wollen, erstellen Sie bitte eine Benutzergruppe. Danach weisen Sie dieser Benutzer-

gruppe entsprechende Rechte zu und fügen dann nur noch die erstellten Benutzer dieser Gruppe hinzu. Damit bekommen alle Gruppenmitglieder die Einstellungen und Rechte der Benutzergruppe.

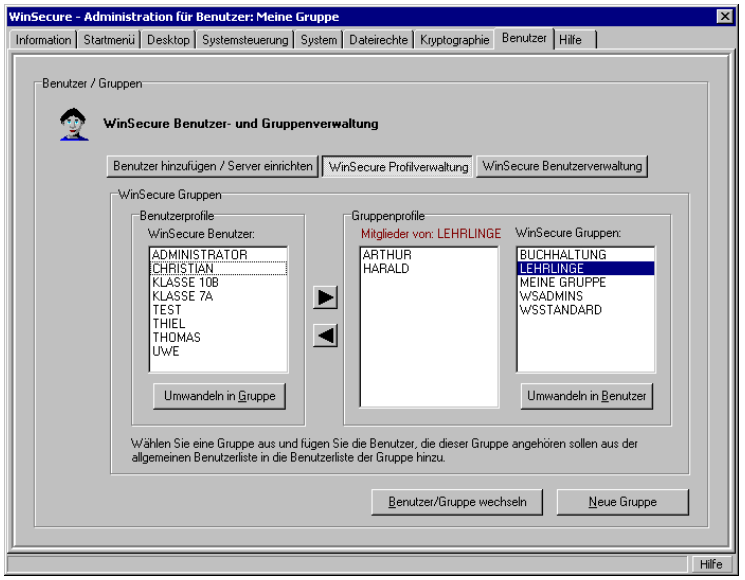


WinSecure® Profilverwaltung

In dem nächsten Bild sehen Sie die WinSecure® Profilverwaltung. Es gibt zwei verschiede Arten von Profilen.

- *Dies sind zum einen Benutzerprofile, die Sie im linken Anzeigefeld sehen. Diese sind hier im Beispiel "KLASSE 10B" und "KLASSE 7A". Ein Benutzer profil gehört zu einem einzigen Anmeldenamen. Jedes Benutzerprofil hat typischerweise seine eigenen Einstellungen.*
- *Zum Zweiten gibt es Gruppenprofile, welche Sie in den beiden rechten Anzei gefeldern sehen. Im rechten Anzeigefeld sehen Sie die hier im Beispiel ange legten vier Gruppen "BUCHHALTUNG", "LEHRLINGE", "MEINE GRUPPE", "WSADMINS" und "WSSTANDARD.*

Mit der Maus können Sie die einzelnen Gruppen markieren. Ist eine Gruppe rechts markiert, werden im mittleren Anzeigefeld dessen Mitglieder angezeigt. In unserem Beispiel gehören also zur Gruppe "LEHRLINGE" die Benutzer "ARTHUR" und "HARALD". Falls im rechten Anzeigefeld eine Gruppe markiert ist, kann man durch Markieren und Drücken der Pfeiltasten Benutzer aus der jeweiligen Gruppe herausnehmen oder von den Benutzerprofilen in das Gruppenprofil mit aufnehmen.



Wenn Sie einen Benutzer im Anzeigefeld "**Benutzerprofile**" markiert haben, können Sie diesen Benutzer mit allen seinen Einstellungen durch Drücken des Buttons "**Umwandeln in Gruppe**" in eine Benutzergruppe umwandeln. Umgekehrt können Sie eine Benutzergruppe durch Drücken des Buttons "**Umwandeln in Benutzer**" in einen Benutzer umwandeln.

Um eine Gruppe in einen Benutzer umwandeln zu können, müssen Sie allerdings zuerst alle Benutzer die der Gruppe angehören aus dieser Gruppe entfernen.

Mit dem Button "**Benutzer/Gruppe wechseln**" können Sie den zu bearbeitenden Benutzer bzw. die Gruppe ändern. Das gerade in Bearbeitung befindliche Benutzerprofil ist "MEINE GRUPPE".

Mit dem Button "**Neue Gruppe**" rufen Sie den Assistenten zur Erstellung einer Benutzergruppe auf. Mit diesem können Sie eine weitere Benutzergruppe anlegen. Wenn Sie eine Gruppe als Kopie eines Benutzers erstellen müssen Sie den erstellten Benutzer durch Klick auf **Umwandeln in Gruppe** nach der Erstellung in eine Gruppe umwandeln.

!! ACHTUNG !!

Eine Sonderstellung unter allen Gruppen nimmt die voreingestellte Gruppe "WSADMINS" ein. Alle Mitglieder der Gruppe WSADMINS können mit Ihrem Konto/Kennwort die Sicherheit von WinSecure® für beliebige Benutzer deaktivieren. Als Benutzersicherheitsprofil wird bei Mitgliedern der WSADMINS-Gruppe immer das persönliche Profil des Benutzers und nicht das Gruppenprofil verwendet.

Aus der Gruppe "WSSTANDARD" werden für die in WinSecure® unbekannten Benutzer mit Sicherheitsprofilen versorgt.

Ein Benutzer, der beispielsweise die Anmeldung abbricht oder ein Benutzer, der nicht in der WinSecure® Benutzerverwaltung gefunden wird, bekommt dieses Sicherheitsprofil.

WinSecure® Benutzerverwaltung

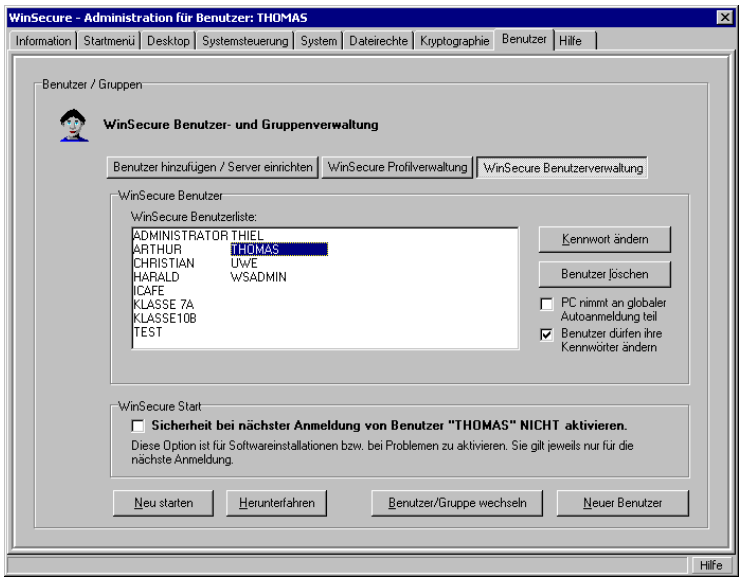
Wenn Sie den Button "WinSecure® Benutzerverwaltung" drücken, können Sie alle in WinSecure® angelegten Benutzer sehen. Nachdem Sie einen Benutzer markiert haben, können Sie mit dem Button "**Kennwort ändern**" dessen Kennwort ändern, mit dem Button "**Benutzer löschen**" diesen löschen.

Ist die Checkbox "**PC nimmt an globaler Autoanmeldung teil**" gewählt (default), so wird sich der PC automatisch anmelden, wenn die globale Autoanmeldung für einen Benutzer gesetzt wurde. Deaktivieren Sie diese Option bei allen PC, die nicht global automatisch angemeldet werden sollen. (z.B. Lehrer-PC in einem Schulungsraum). Diese Option ist PC-gebunden und muss auf jedem PC eingestellt werden. Die globale Autoanmeldung funktioniert nur, wenn ein WinSecure®-Server im Einsatz ist.

Ist die Checkbox "**Benutzer dürfen Ihre Kennwörter ändern**" gewählt (default), so erhalten die Benutzer im Anmeldedialog die Möglichkeit ihr Kennwort zu ändern.

Diese Option ist PC-gebunden und muss auf jedem PC eingestellt werden.

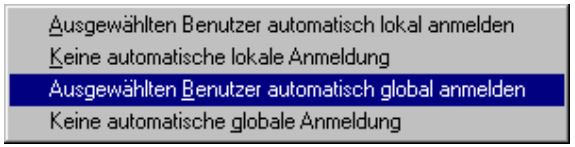
Falls Sie ein Häkchen in die Checkbox "**WinSecure Start**" gesetzt haben, wird WinSecure® beim **nächstfolgenden** Anmelden dieses Benutzers **nicht** gestartet. Dies ist dann notwendig, wenn Sie Software auf dem Computer installieren und diese Software die Installation erst nach einem erneuten Neustart fertigstellt. Wenn Sie dieses Häkchen in einem solchen Fall vergessen, wird das Konfigurationsprogramm der neuen Software von WinSecure® abgewiesen und sie bekommen Fehler bei der Installation.



Mit dem Button "Benutzer/Gruppe wechseln" können Sie die Gruppe oder den Benutzer wechseln, mit dem Button "Neuer Benutzer" können Sie den Assistent zum Erstellen eines Benutzers aufrufen.

Die beiden Buttons **"Neu starten"** und **"Herunterfahren"** sind speziell für den Einsatz in Schulungsräumen gedacht. Sind mehrere Clients an einem WinSecure® Server angemeldet, können mit dem Drücken des Buttons "**Herunterfahren**" alle anderen Rechner heruntergefahren werden. Mit dem Drücken des Buttons "**Neu starten**" alle anderen Rechner außer des eigene PC herunter gefahren und neu gestartet werden.

Außerdem können Sie mit Winsecure® veranlassen, dass sich ein beliebiger Benutzer automatisch an einem bestimmten Rechner oder aber an allen Stationen automatisch anmeldet, auf denen die Option "**PC nimmt an globaler Autoanmeldung teil**" aktiviert ist. Dies ist insbesondere für den Schulungsbetrieb sehr nützlich. Sie sehen, dass bereits zwei Benutzer mit den Namen "KLASSE 10B" und "KLASSE 7A" bestehen. Für diese beiden Benutzer haben wir vorher diejenigen Programme und Sicherheitseinstellungen definiert, welche die beiden Schulklassen ausführen dürfen. Wenn Sie jetzt einen der beiden Benutzer markieren und die rechte Maustaste klicken, bekommen Sie folgendes Auswahlfenster:

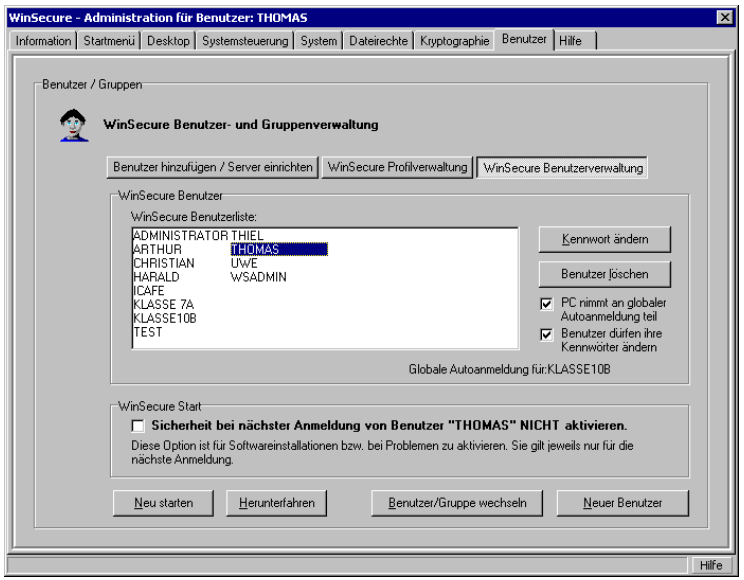


Wenn Sie den Eintrag wie im Beispiel auswählen, wird Ihnen in der Administration angezeigt, dass Sie eine globale Autoanmeldung für den Benutzer “KLASSE 10B” gesetzt haben.

Definieren Sie also zuerst für alle Schulungsgruppen jeweils einen Benutzer und dessen Einstellungen. Vor dem Unterrichtsbeginn setzen Sie eine globale Anmeldung für die entsprechende Gruppe und beim Hochfahren der Schulungsrechner wird ohne Hinzutun der Schulungspersonen automatisch der gewählte Benutzer angemeldet.

Neben der globalen Autoanmeldung gibt es die lokale Autoanmeldung, die nur für den jeweiligen PC gilt. Die lokale Autoanmeldung arbeitet sowohl in einem WinSecure®-Netzwerk mit WinSecure®-Server als auch auf Stand-Alone-Clients

Beim Ende der Schulungsstunde können Sie mit den Buttons “**Neu starten**” bzw. “**Herunterfahren**” alle Rechner beenden.



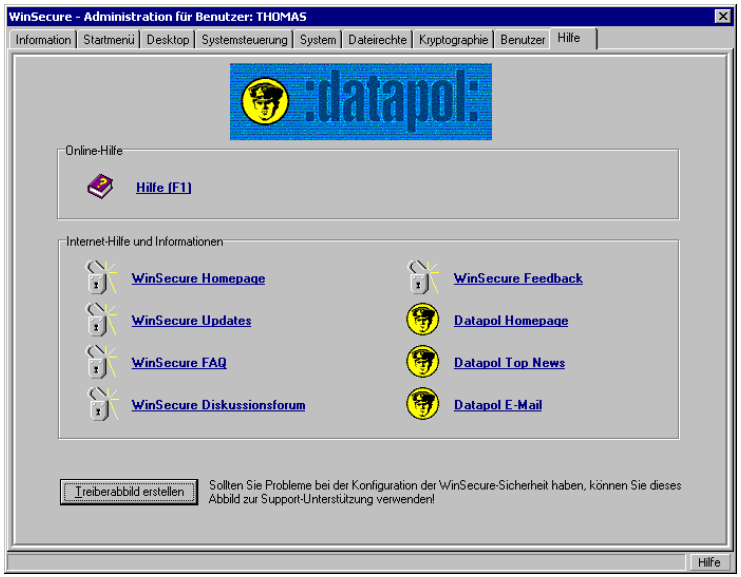
Achtung:

Die lokale Autoanmeldung hat eine höhere Priorität als die globale Autoanmeldung.

4.10. Der Reiter Hilfe

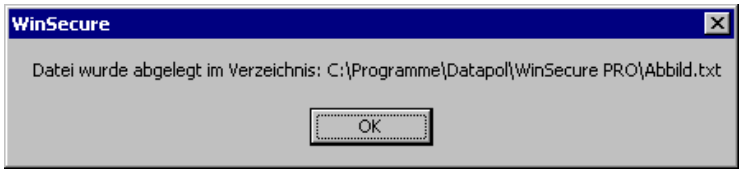
Im Reiter “**Hilfe**” können Sie die Online-Hilfe aufrufen. Außerdem können Sie die Online Hilfe auch jederzeit mit der Taste F1 erreichen.

Falls Sie einen Internetzugang haben, können Sie auch die anderen Auswahlpunkte der Hilfe benutzen. Sie kommen dann zur Homepage von WinSecure® und können sich über Produktupdates informieren, die FAQs von WinSecure® ansehen oder sich im WinSecure® Diskussionsforum mit anderen Anwendern austauschen. Mit den anderen Auswahlpunkten können Sie per E-Mail mit dem WinSecure® Team direkt in Kontakt treten und sich auch über weitere interessante Softwareprodukte der Datapol GmbH informieren.



Bitte beachten Sie im Reiter “**Hilfe**” unbedingt auch den Button “**Treiberabbild erstellen**”. Diese Funktion erlaubt Ihnen, ein Treiberabbild über Ihre aktuellen Sicherheitseinstellungen zu erstellen. Das “**Treiberabbild**” ist eine Textdatei, die hauptsächlich zu Supportzwecken dient und verdeutlicht, welche Attribute für die verschiedenen Laufwerke, Verzeichnisse und Dateien gesetzt sind.

Näheres über den Filetreiber finden Sie im Kapitel “Grundeinstellung des WinSecure® Filetreibers”.



4.11. Der Benutzer WSADMIN

Eine Sonderstellung unter allen Benutzern nimmt der WinSecure®-Administrator "**WSADMIN**" ein. Dieser Benutzer kann nicht gelöscht werden.

Als Benutzer WSADMIN haben die Möglichkeit, die Sicherheit eines beliebigen Benutzers zu deaktivieren, den Scanmode zu aktivieren, das Logfile bei aktivierter Sicherheit zu lesen und allen anderen Sicherheitsfunktionen in WinSecure® zu bedienen und zu administrieren.

Weiterhin ist der Benutzer WSADMIN der einzige Benutzer, der bei einer Windows-Anmeldung nicht den automatischen Start von WinSecure® zur Folge hat. Wenn also Probleme beim Start von Windows auftreten, so können Sie immer den Benutzer WSADMIN anmelden und dann ohne jegliche Sicherheitseinstellungen von WinSecure® arbeiten.

Unter Windows 95/98/ME finden Sie in der Administration des Benutzers WSADMIN die Möglichkeit den Schutz des Bootvorganges zu deaktivieren.

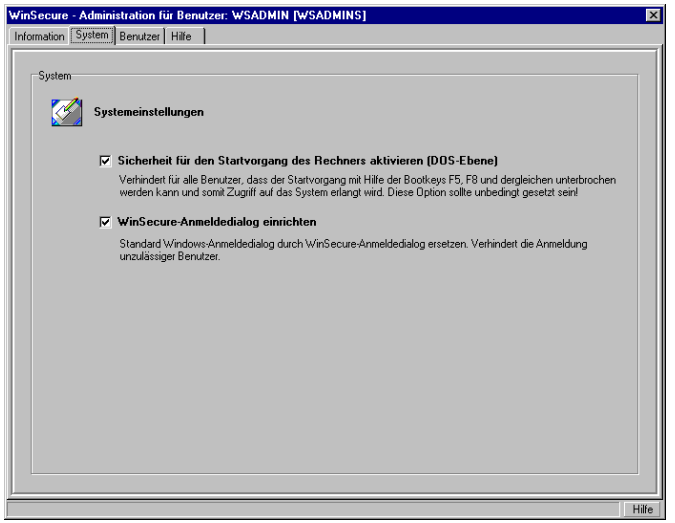
Zu diesem frühen Zeitpunkt des Startvorganges des Rechners ist allerdings WinSecure® noch nicht in den Speicher geladen, so dass sich WinSecure® hier einer Windows Funktion bedient. WinSecure® öffnet die Datei "msdos.sys" und trägt dort die Zeile "BootKeys=0" ein. Dieser Eintrag ist für die Hardware die Anweisung, die Bootkeys abzuschalten. Wenn Sie Probleme haben, schauen Sie bitte zuerst in diese Datei. Sie können diesen Eintrag auch von Hand vornehmen. In sehr seltenen Fällen funktioniert dieses Verfahren nicht. In diesem Fall ist Ihr System nicht zu 100% Windows kompatibel.

ACHTUNG:

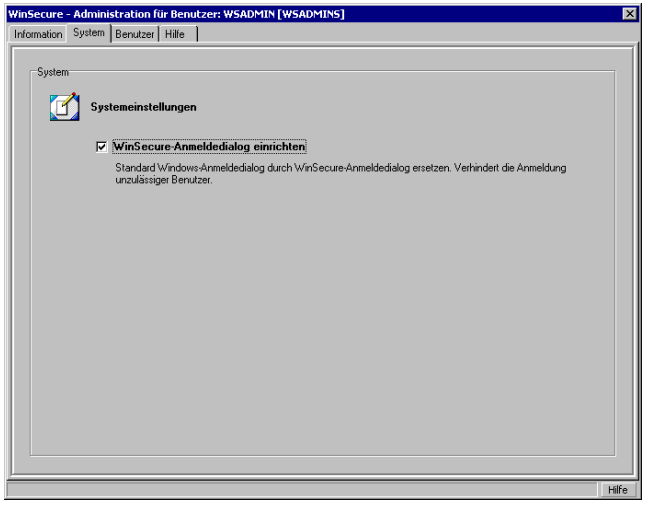
Diese Option sollte unter Windows 95/98/ME immer gesetzt sein! Damit wird verhindert, dass ein Benutzer den Start von Windows abbricht und so in den MS-DOS-Modus gelangt.

Des weiteren kann hier mit einer Checkbox eingestellt werden, ob WinSecure® seinen mitgelieferten und sicheren Anmeldebildschirm verwenden soll oder nicht.

Unter Windows 95, 98, ME sieht der Reiter wie folgt aus.



In Windows NT, Windows 2000 und Windows XP wird in diesem Reiter lediglich der Anmeldedialog zur Konfiguration angezeigt.



5. Arbeiten mit Gruppen

In großen Netzwerken kann es sehr umständlich sein, für jeden Benutzer ein WinSecure® Profil zu erstellen. Auch die Pflege von sehr vielen Benutzern kann durch den Einsatz von Gruppen stark vereinfacht werden.

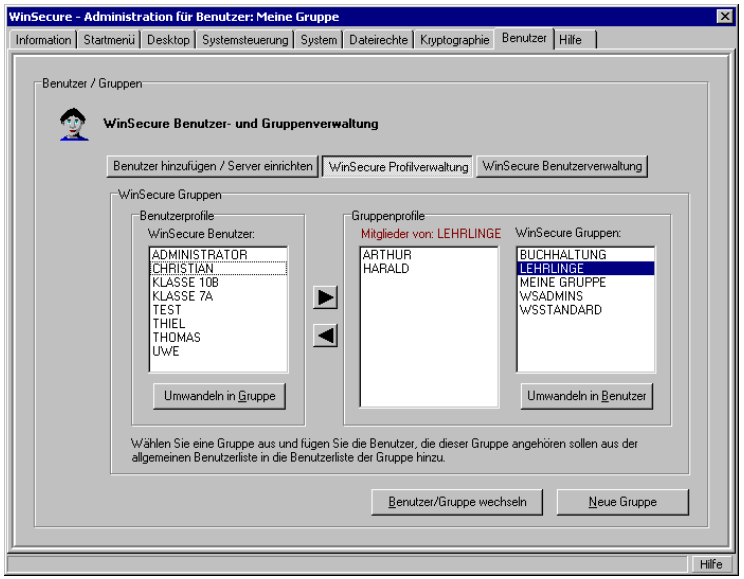
Unterschiede zu Gruppen unter Windows NT

Zur Zeit ist es nicht möglich, in WinSecure® die Gruppenfunktionalität von Windows NT zu nutzen. Das liegt daran, dass ein Benutzer zwar Mitglied mehrer Gruppen in Windows NT sein kann, jedoch immer nur exakt ein Sicherheitsprofil besitzen kann.

5.1. Anlegen einer Gruppe

Bevor Sie einzelne Benutzer einer Gruppe hinzufügen können, müssen Sie zuerst eine “Benutzergruppe” anlegen.

Öffnen Sie dazu die WinSecure® Administration. Gehen Sie zum Reiter “**Benutzer**” und dort in die “**WinSecure® Profilverwaltung**”.



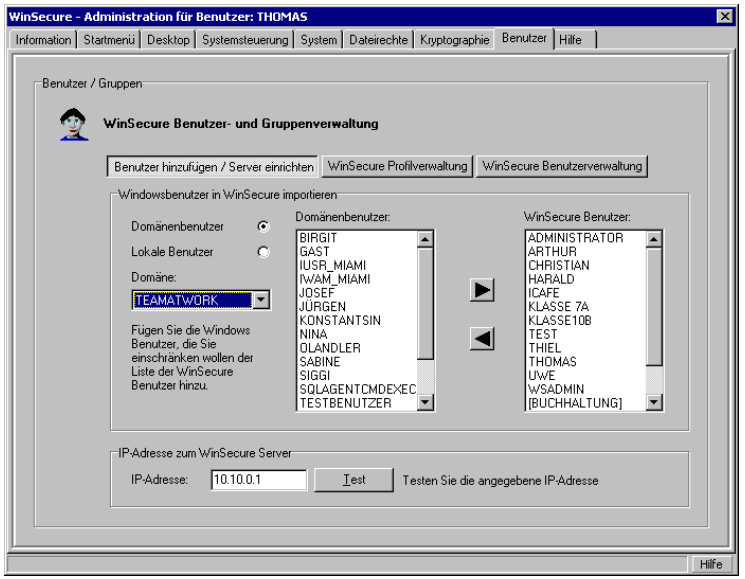
Klicken Sie hier bitte auf “**Neue Gruppe**”. Es folgt der Assistent zum Anlegen neuer Gruppen. Folgen Sie den Anweisungen auf dem Bildschirm.

Wiederholen Sie diesen Vorgang für alle Gruppen, die Sie anlegen möchten.

5.2. Importieren von Benutzern

Damit Sie nicht jeden Benutzer manuell importieren müssen, stellt Ihnen WinSecure® mehrere Möglichkeiten zur Verfügung, Benutzer zu importieren.

Alle bekannten lokalen Benutzer sowie die Benutzer bekannter Domänen können im Reiter “**Benutzer**” importiert werden.

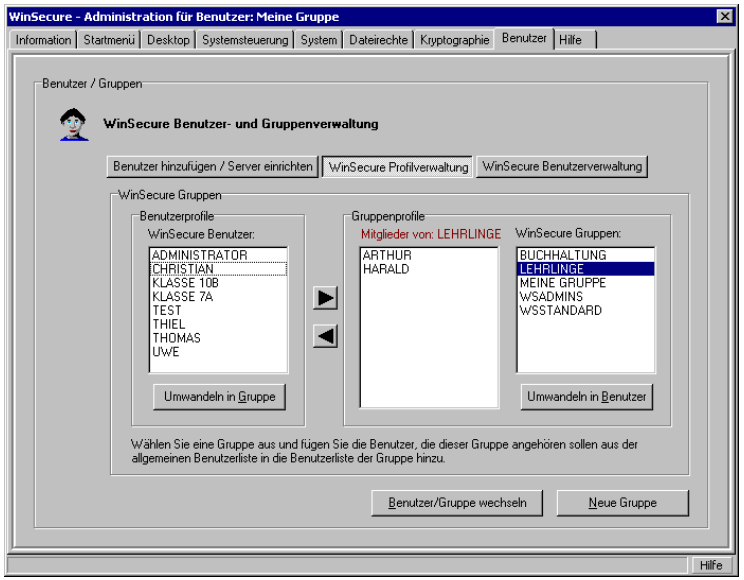


5.3. Hinzufügen von Benutzern zu einer Gruppe

Im Reiter Benutzer können Sie in der Profilverwaltung eingerichtete Benutzer zu einer Gruppe hinzufügen.

Wählen Sie dazu rechte die Gruppe (z.B. Lehrling) aus und markieren Sie links die Benutzer, die Sie der Gruppe hinzufügen wollen. Mit dem Button  können Sie die Benutzer dann der markierten Gruppe hinzufügen.

Um Benutzer aus einer Gruppe zu entfernen verfahren Sie analog und klicken auf den Button 



5.4. Die Gruppe WSADMINS

Eine **Sonderstellung** unter allen Gruppen nimmt die vordefinierte Gruppe **WSADMINS** ein.

Diese Gruppe kann nicht gelöscht werden.

Alle Mitglieder der Gruppe "**WSADMNS**" können mit Ihrem Konto und Kennwort die Sicherheit deaktivieren. Damit auch verschiedene Administratoren mit unterschiedlichen Sicherheitsprofilen arbeiten können, erhalten alle Mitglieder der Gruppe WSADMINS das Benutzer- und nicht das Gruppenprofil bei der Anmeldung zugeteilt.

Der Benutzer WSADMIN ist ebenfalls Mitglied der Gruppe WSADMINS und kann aus dieser Gruppe auch nicht entfernt werden. Im Gegensatz zu allen anderen Mitgliedern der Gruppe WSADMINS wird bei einer Anmeldung des Benutzers WSADMIN die Sicherheit **NIEMALS** aktiviert.

Aus diesem Grund sollten Sie alle Benutzer der Benutzergruppe **WSADMINS** sehr sorgfältig auswählen und auf jeden Fall für jeden Benutzer dieser Gruppe ein sehr sicheres Kennwort wählen.

Wenn Sie importierte Benutzer später zur Gruppe WSADMINS hinzufügen, sollten Sie evtl. deren Kennwörter ebenfalls ändern und sie gegebenenfalls mit den Kennwörtern unter Windows NT gleichsetzen.

Da alle WinSecure® Administratoren jederzeit ihre Kennwörter ändern können auch **OHNE** die alten Kennwörter zu kennen, ist es ratsam, nur wenigen Personen Administrationsrechte für WinSecure® zu erteilen.

5.5. Die Gruppe WSSTANDARD

Die Gruppe "WSSTANDARD" stellt ebenfalls eine Sondergruppe dar. Sie existiert bereits nach den Installation.

Dieser Gruppe können wie bei jeder anderen Gruppe auch Sicherheitseinstellungen zugewiesen werden. Die Besonderheit bei dieser Gruppe ist, dass alle unbekannten Benutzer mit den Sicherheitseinstellungen dieser Gruppe versorgt werden.

6. Arbeiten mit Datentresoren

Datentresore in WinSecure sind grundsätzlich sehr sicher. Viele herkömmliche Programme verwenden oft sehr kurze Passwörter um dem Benutzer den Zugang zu den verschlüsselten Daten zu erleichtern. WinSecure dagegen verwendet einen sehr langen Schlüssel in Kombination mit einem kurzen benutzerfreundlichen Passwort. Dadurch wird effektiv verhindert, dass mit sogenannten Brute-Force-Angriffen das Kennwort des Datentresors geknackt werden kann.

Sollte jemand die Festplatte Ihres PCs ausbauen und über einen zweiten PC versuchen den Schlüssel des Datentresors zu knacken, so müsste er dazu bei heutiger Rechnerleistung viele Jahre aufwenden.

6.1. Funktionsweise des Datentresors

Ein WinSecure® Datentresor stellt ein virtuelles Laufwerk dar, das auf einem physischen Laufwerk “gehostet” wird. Diese Technologie kennen Sie vielleicht bereits. Sie wird u.a. auch von Doublespace verwendet wird (dort allerdings zum komprimieren von Daten).

Auswahl des Speicherortes für einen Datentresor:

Datentresore können Sie entweder auf einer lokalen Festplatte des jeweiligen PC oder auf einem verbunden Netzwerklaufwerk erstellen. Beachten Sie bitte, dass Datentresore, die auf einer lokalen Festplatte erstellt wurden **NICHT** von einem anderen PC aus geöffnet werden können. Unter Windows NT, Windows 2000 und Windows XP können Datentresore NUR auf lokalen Laufwerken erstellt werden!

Wodurch unterscheidet sich ein geöffneter Datentresor von einem gewöhnlichen Laufwerk?

Erst einmal natürlich dadurch, dass der Inhalt des Datentresors verschlüsselt ist. Ansonsten aber sind Datentresore genau gleich zu behandeln wie lokale oder verbundene Datenträger.

Der Datentresor wird als FAT-Laufwerk implementiert.

Die Details der einzelnen Verschlüsselungsmöglichkeiten:

-BlowFish

Ist eine symmetrische Blockverschlüsselung mit einer variablen Keylänge von 32-448 Bits. Blowfish wurde erstmalig von Bruce Schneier 1993 vorgestellt und gilt als sehr sichere Methode um Daten zu verschlüsseln.

-3DES

Ist die dreifache DES-Verschlüsselung von Diffie & Hellman. Diese Verschlüsselung verwendet einen 168 Bit Schlüssel, gilt als sehr sicher aber auch als relativ langsam.

-WSummer

Ist eine auf maximale Geschwindigkeit ausgelegte Verschlüsselungsvariante mit einem 128 Bit Schlüssel.

6.2. Umgang mit Kennwörtern

Jeder Datentresor, der mit WinSecure® erstellt wurde, verfügt über zwei Kennworte:

Das Masterkennwort

ist ein zufallsgeneriertes Kennwort, das nur zur Wiederherstellung eines Datentresors verwendet werden kann, bzw. um ein vergessenes Kennwort für einen Datentresor zu ändern. Dieses Kennwort müsste ein Hacker knacken, um an die gesicherten Daten heranzukommen. Zudem muss er die verwendete Verschlüsselungsart kennen. Das Masterkennwort benutzt mehr als 20 Zeichen aus dem vollen Zeichensatz und bietet damit mindestens 10 hoch 48 mögliche Kombinationen. (zum Vergleich: Seit dem Urknall sind ca. 10 hoch 18 Sekunden vergangen...)

Das Benutzerkennwort

ist das Kennwort, mit dem der Benutzer seinen Datentresor öffnen kann. Dieses Kennwort kann vom Benutzer geändert werden. Das Benutzerkennwort kann nur durch “try and error” erraten werden, wenn kein Brute-Force-Programm zugelassen wurde. Damit sind Sie bereits mit 4-6 Zeichen relativ sicher. Wir empfehlen Ihnen trotzdem eine willkürliche Kombination aus Buchstaben, Zahlen und Sonderzeichen für dieses Benutzerkennwort zu verwenden. Namen, Geburtstage etc. sollten Sie nicht verwenden, da diese relativ leicht erraten werden können.

Typische Vorgehensweise

Der WinSecure® Administrator erstellt im Beisein des Datentresoranwenders einen Datentresor. Der Masterschlüssel wird dabei auf eine Diskette gespeichert und versiegelt an einem sicheren Ort aufbewahrt.

Der Anwender ändert sein Benutzerkennwort für den Datentresor direkt nach der Einrichtung des Tresors durch einen Klick mit der linken Maustaste auf das geschlossene WinSecure-Schloss in der Taskleiste.

Vergessenes Benutzerkennwort

Wenn der Anwender sein Benutzerkennwort vergessen hat, kann ihm der Administrator unter Verwendung der Masterdiskette ein neues Kennwort vergeben.

Neuinstallation eines PC mit Datentresor

Muss ein PC neu installiert werden, so muss das Datentresor-File (i.d.R. Benutzername.cry) von einer bestehenden Datensicherung wieder auf den PC kopiert werden. Um erneut Zugriff auf den Datentresor zu erhalten, erstellen Sie einen neuen Datentresor an exakt der gleichen Position und mit exakt dem gleichen Namen wie der alte Tresor. Sie werden dann aufgefordert die Masterdiskette einzulegen um den alten Datentresor wiederherzustellen.

7. WinSecure® korrekt deinstallieren

WinSecure® verfügt über ein **eigene** Deinstallations-Routine.

Verwenden Sie keine kommerziellen Uninstaller für die Deinstallation von WinSecure® !

Andere Deinstaller können eventuell nicht alle Programmteile löschen und dadurch das System in einem nicht brauchbaren Zustand zurücklassen, da WinSecure® Systemdateien in einer Art verändert, die normale Uninstaller nicht verarbeiten können.

Verwenden Sie also immer das von der Datapol GmbH mitgelieferte Deinstallationsprogramm.

Bevor Sie mit der Deinstallation von WinSecure® beginnen, beenden Sie WinSecure® durch einen Klick mit der rechten Maustaste auf das geöffnete Schloss-Icon rechts unten am Bildschirm. Wählen Sie dann die Option „**WinSecure® beenden**“. Alternativ hierzu können Sie sich aber auch nachdem Sie sich abgemeldet haben als Benutzer „WSADMIN“ anmelden.

Beim Benutzer „WSADMIN“ wird WinSecure® generell nicht gestartet und kann damit problemlos mit dem WinSecure® Deinstaller deinstalliert werden.

Danach starten Sie im Startmenü - Programme - WinSecure - WinSecure entfernen.

Das Deinstallationsprogramm wird alle Einstellungen in den ursprünglichen Zustand versetzen.

Nach dem erforderlichen Neustart werden dann die übrigen Dateien vom System entfernt.

WinSecure® ist damit komplett deinstalliert.

8. WinSecure um Funktionen erweitern

Sicherheit ist ein sehr komplexes Thema. Daher kann es vorkommen, dass Sie bestimmte Sicherheitsfunktionen zu WinSecure® hinzufügen möchten.

Zu diesem Zweck haben wir in WinSecure® eine Schnittstelle zur Registry von Windows eingebaut.

!! Achtung !!

Die im folgenden beschriebenen Vorgänge sollten NUR von fachlich ausgebildeten Administratoren durchgeführt werden. Änderungen an der Registry können zur Beschädigung des Systems führen und eine Neuinstallation erforderlich machen.

Bevor Sie die unten beschriebenen Dateien zum Einsatz bringen sollten Sie dies vorher gründlich testen!

Besondere Sorgfalt gebührt hierbei dem Einsatz unter Windows NT und Windows 2000, da ein gewöhnlicher Benutzer unter diesen Betriebssystemen keinen Zugriff auf die Policy-Einstellungen unter HKEY_CURRENT_USER erhält und Sie daher lediglich Policies unter HKEY_LOCAL_MACHINE verwenden können bzw. alle Benutzer lokal über Administratorrechte verfügen müssen.

8.1. Beschreibung der Schnittstelle

Wenn Sie selbst Änderungen an der Registry definieren wollen, die automatisch bei der Aktivierung der Sicherheit vorgenommen werden sollen, müssen Sie zwei Reg-Files erzeugen und diese Lock.reg und Unlock.reg benennen und dann in das Programmverzeichnis von WinSecure® kopieren.

Was ist ein Reg-File?

Regfiles können automatisch erzeugt werden in dem Sie in Registryeditor „regedit.exe“ den Befehl „Exportieren“ ausführen.

Eine ASCII-Datei beschreibt die gewählten Einträge der Registry.

Aufbau eines RegFiles

Ein RegFile hat immer den folgenden Aufbau:

REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
„NoClose“=dword:00000001
„NoLogOff“=dword:00000001
„NoRun“=dword:00000001
„NoFind“=dword:00000001
„NoSetFolders“=dword:00000001
„NoSetTaskbar“=dword:00000001
„NoWindowsUpdate“=dword:00000001
„NoFavoritesMenu“=dword:00000001
„NoRecentDocsMenu“=dword:00000001
„NoRecentDocsHistory“=dword:00000001
„NoChangeStartMenu“=dword:00000001
„NoSetActiveDesktop“=dword:00000001
„NoTrayContextMenu“=dword:00000001

Dabei beschreibt die erste Zeile *REGEDIT4* die Version des eingesetzten Registrierungseditors. Sie kommt nur einmal am Anfang des Reg-Files vor.

Die nächste Zeile
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer] beschreibt den Pfad, unter dem die darunter aufgeführten Einträge eingetragen werden sollen.

Die folgenden Zeilen wie z.B. *„NoClose“=dword:00000001* fügt einen Eintrag NoClose mit dem DWORD-Wert „1“ hinzu. (Dieser Eintrag z.B. verhindert, dass der Benutzer den PC über das Startmenü beenden kann.

Zusammenfügen mehrer RegFiles

wenn Sie mehrere einzelne RegFiles erzeugt haben und diese zu einer zusammenfügen möchten, so kopieren Sie den Inhalt der zweiten Datei ohne die erste Zeile *REGEDIT4* und fügen Sie an die erste Datei an. So können Sie beliebig viele RegFiles zu einer einzigen zusammenfügen.

Funktion der Datei Lock.Reg

Alle Einstellungen der Datei Lock.reg werden beim Aktivieren der Sicherheit importiert und direkt angewendet. Sie sollten deshalb in dieser Datei alle Einstellungen treffen, die zur Einschränkung des Benutzers dienen.

Funktion der Datei Unlock.Reg

Alle Einstellungen der Datei Unlock.reg werden beim Deaktivieren der Sicherheit importiert und direkt angewendet. Sie sollten deshalb in dieser Datei alle Einstellungen die Sie in der Lock.reg getroffen haben wieder zurücksetzen. Normalerweise erreichen Sie dies indem Sie die Einträge von „1“ auf „0“ umschreiben. Eine schnelle Art die Datei Unlock.reg zu erzeugen ist deshalb die Datei Lock.reg zu editieren, alle Einträge umzuschreiben und sie dann unter dem Namen Unlock.reg zu speichern.

8.2. Besonderheiten unter Win95/WinNT4

Einige Einstellungen werden unter Windows 95 und Windows NT4 nicht zur Laufzeit übernommen.

Installieren Sie in diesem Fall einen Internet Explorer ab Version 5.5 (ist auf der WinSecure®-CD enthalten) mit den Desktoperweiterungen.

Nach der Installation sollten die Änderungen bei der Aktivierung und Deaktivierung der Sicherheit automatisch übernommen werden.

8.3. Startmenü einschränken

Falls Sie das Startmenü von Windows über RegFiles oder über WinSecure® eingeschränkt haben, benötigt Windows in einigen Fällen bis zu 30 Sekunden Zeit, um das Startmenü umzubauen.

Klicken Sie während dieser Zeit nicht auf den Start-Button, da ansonsten das Startmenü nicht mehr umgebaut wird sondern in der aktuellen Version im Datenzwischenspeicher (Cache) gespeichert bleibt.

Die Möglichkeiten, das Startmenü einzuschränken hängen vom eingesetzten Betriebssystem ab. Unter Windows 95, Windows 98 und Windows NT4 ist es beispielsweise i.d.R. nicht möglich, die Hilfe-Funktion aus dem Startmenü auszublenden.

8.4. Weiteres Customizing

Andere Anpassungsmöglichkeiten bestehen z.B. darin, den Anmeldedialog um Fingerprint Scanner oder SmartCards zu erweitern. Diese Möglichkeiten erfordern programmtechnische Änderungen und können nur von autorisierten WinSecure® Competenz-Centern durchgeführt werden.

WinSecure® API

Die WinSecure® API stellt eine leistungsfähige und leicht zu implementierende Schnittstelle zur RBCD-Technologie zur Verfügung. Falls Sie anstatt der kompletten Funktionalität von WinSecure® nur an der Möglichkeit interessiert sind, Verzeichnisse und Dateien (auch mit WildCards und Jokern) mit beliebigen Rechten zu versehen, so können Sie mit der WinSecure®-API in Minuten z.B. wichtige Files der Warenwirtschaft gegen Löschen oder Umbenennen schützen.

Für weitere Informationen zur WinSecure-API kontaktieren Sie unseren Vertrieb unter sales@datapol.de bzw. unter T: 07352-9222-0.

Krypto-API

Auch die Funktionalität der Datentresore kann in Form einer API zur Verfügung gestellt werden. Sie können damit direkt in Ihrer Anwendung Datentresore erstellen und anwenden.

9. Liste läufig gestellter Fragen

Sie finden eine aktualisierte Liste der häufigst gestellten Fragen auf unserer WebSite http://www.winecure.de

9.1. Unter Windows95/98/Millennium

Warum kann ich das Systemlaufwerk, auf dem Windows installiert ist nur verstecken?

Das Systemlaufwerk kann nicht gesperrt werden, da Windows selbst temporär Dateien auf die Festplatte ablegt und deshalb Schreibzugriff auf dieses Laufwerk gewährt werden muss. Bestimmte Dateien im Betriebssystem sind aber trotzdem geschützt und können nicht gelöscht oder verändert werden. Wenn Sie sich ein Treiberabbild erstellen lassen, sehen Sie darin, welche Dateien WinSecure® standardmäßig schützt.

Ein zugelassenes Programm startet nicht. Was kann ich tun?

Sie haben ein Programm zugelassen, das sich nicht mehr auf der Festplatte oder nicht an der angegebenen Stelle befindet. Kontrollieren Sie bitte, ob das entsprechende Programm noch genau dort zu finden ist, wo es bei der Einrichtung installiert. Eventuell ist das entsprechende Programm auch auf einem gesperrten Laufwerk installiert. In diesem Fall müssten Sie das gesperrte Laufwerk freigeben.

Nach der Anmeldung stürzt Windows mit Fehler XY ab. Muss ich neu installieren?

Melden Sie sich als Benutzer „WSADMIN“ an. Für diesen Benutzer wird WinSecure® nie gestartet und Sie haben so die Möglichkeit, die Fehlkonfiguration zu beheben.

Wodurch unterscheidet sich Test- und Vollversion?

Wenn Sie keine Lizenzdiskette besitzen wird Ihnen am Client angezeigt, dass Sie eine nicht lizenzierte Version besitzen. In der Testversion unterliegen Sie keinerlei Einschränkungen. Allerdings erscheinen regelmäßig Meldungen die Sie daran erinnern, dass Sie eine nicht lizenzierte Version benutzen.

Ich habe im Startmenü trotz Restriktionen immer noch alle Programme angezeigt bekommen. Was mache ich falsch?

In seltenen Fällen kann dies auftreten, wenn Programme wie beispielsweise Norton Utilities installiert sind. Diese halten das Startmenü in einem Cache-Speicher. Allerdings werden die Programme nur angezeigt und können nicht ausgeführt werden. Um den Fehler zu beseitigen, müssen Sie diese Utilities deinstallieren.

Nach der Deinstallation meldet sich nicht mein gewohnter Microsoft NT oder Novell Anmeldedialog. Wie setze ich dies zurück?

Stellen Sie den Microsoft-Client oder Novell-Client Anmeldedialog als ersten Anmeldedialog ein. Dies können Sie unter Systemsteuerung/Netzwerk unter „**Primäre Netzwerkanmeldung**“ einstellen. Dort wählen Sie lediglich Ihren Microsoft- oder Novell-Anmeldedialog aus.

Meine automatisch gestarteten Programme werden alle beim Booten abgewiesen. Wie kann ich diese zulassen?

Sie können diese Dateien unter Verwendung des Logfiles zur Liste der erlaubten Programme hinzufügen. Näheres finden Sie im Abschnitt „**Dateien zulassen**“.

Nach der Installation einer Anwendung stürzt Windows beim Anmeldedialog mit einer Fehlermeldung ab. Ich kann mich auch als Administrator nicht mehr anmelden. Wie kann ich diesen Fehler beheben?

Die Logon-Provider von WinSecure® wurden beschädigt. Booten Sie Ihren PC mit einer Startdiskette und löschen Sie dann im Verzeichnis C:\Windows\System die Dateien „**wsnett.dll**“ und „**wsnetp.dll**“. Starten Sie nun wie gewohnt den PC (es werden Fehlermeldungen auftreten). Wenn Windows gestartet ist, starten Sie bitte das WinSecure® Setup für Windows 95/98/ME. Ihre Einstellungen bleiben erhalten. Wenn dies nicht zum gewünschten Ergebnis führt wiederholen Sie den Vorgang und spielen Sie die WinSecure®-Lizenz zurück. Danach müssen Sie Windows reparieren oder neu installieren, bevor Sie WinSecure® erneut installieren. Der Fehler ist in diesem Fall auf eine beschädigte Windows-Installation zurückzuführen.

Nach der Installation von WinSecure® wird zwar das Schloß rot, aber trotzdem kann ich alle Dateien ausführen. Wie kann ich diesen Fehler beheben?

In Ihrem System ist ein Treiber installiert, der die I/O Schiene falsch behandelt bzw. einen Hook dort setzt. Dies kann entweder durch ein Utility oder einen Treiber verursacht werden. Bisher bekannt ist lediglich ein alter SCSI-Treiber für einen Tecmar-SCSI-Controller. Deinstallieren Sie diese Treiber oder fragen Sie den jeweiligen Hersteller nach einer fehlerbereinigten Version des Treibers.

In der Version 2.0 von WinSecure® gab es die Möglichkeit den Internet Explorer einzuschränken. Wie mache ich dies in der Version 3.0?

Sie können den Internet Explorer über die Dateien „**Lock.reg**“ und „**Unlock.reg**“ selbst einschränken. Weitere Informationen zur Beschränkung des Internet Explorers finden Sie im IEAK von Microsoft und auf unserer WebSite http://www.winsecure.de

9.2. Unter Windows NT/2000/XP

Warum kann ich das Systemlaufwerk, auf dem Windows installiert ist nur verstecken?

Das Systemlaufwerk kann nicht gesperrt werden, da Windows selbst temporär Dateien auf die Festplatte ablegt und deshalb Schreibzugriff auf dieses Laufwerk gewährt werden muss. Bestimmte Dateien im Betriebssystem sind aber trotzdem geschützt und können nicht gelöscht oder verändert werden. Wenn Sie sich ein Treiberabbild erstellen lassen, sehen Sie, welche Dateien WinSecure® standardmäßig schützt.

Ein zugelassenes Programm startet nicht. Was kann ich tun?

Sie haben ein Programm zugelassen, das sich nicht mehr auf der Festplatte oder nicht an der angegebenen Stelle befindet. Kontrollieren Sie bitte, ob das entsprechende Programm noch genau dort zu finden ist, wo es bei der Einrichtung installiert. Eventuell ist das entsprechende Programm auch auf einem gesperrten Laufwerk installiert. In diesem Fall müssten Sie das gesperrte Laufwerk freigeben.

Wodurch unterscheidet sich Test- und Vollversion?

Wenn Sie keine Lizenzdiskette besitzen wird Ihnen am Client angezeigt, dass Sie eine nicht lizenzierte Version besitzen. In der Testversion unterliegen Sie keinerlei Einschränkungen. Allerdings erscheinen regelmäßig Meldungen die Sie daran erinnern, dass Sie eine nicht lizenzierte Version benutzen.

Meine automatisch gestarteten Programme werden alle beim Booten abgewiesen. Wie kann ich diese zulassen?

Sie können diese Dateien unter Verwendung des Logfiles zur Liste der erlaubten Programme hinzufügen. Näheres finden Sie im Abschnitt Dateien zulassen.

Trotz mehrfachen Versuchs meldet WinSecure® dass das Kennwort für mein Kryptolaufwerk falsch sei. Was kann ich tun?

Sie haben das Hostfile für die Kryptodisk auf einem gesperrten Laufwerk abgelegt. Deshalb kann das Kryptolaufwerk nicht geöffnet werden. Geben Sie das Laufwerk frei oder legen Sie das Hostfile auf einem nicht gesperrten Laufwerk ab.

In der Version 2.0 von WinSecure® gab es die Möglichkeit den Internet Explorer einzuschränken. Wie mache ich dies in der Version 3.0?

Sie können den Internet Explorer über die Dateien „**Lock.reg**“ und „**Unlock.reg**“ selbst einschränken. Weitere Informationen zur Beschränkung des Internet Explorers finden Sie im IEAK von Microsoft und auf unserer WebSite http://www.winsecure.de

In Windows 95/98 kann der Start im abgesicherten Modus verhindert werden. Ich vermisse diese Funktion unter Windows 2000. Wie kann ich den Start mit „F8“ unter Windows 2000 verhindern?

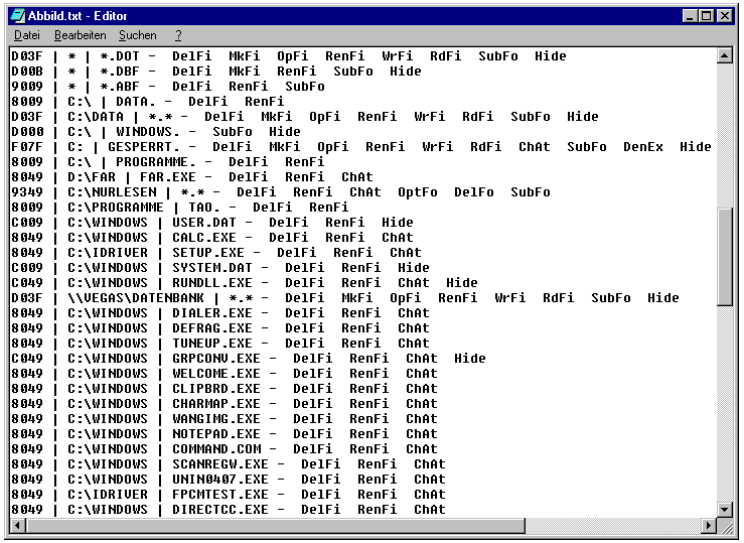
Da der Start im abgesicherten Modus unter Windows 2000 fest in der Datei NTLDR implementiert ist, kann WinSecure® leider keinen Einfluss auf das Startverhalten von Windows 2000 darstellen. Auch wir erachten dies als eine eklatante Sicherheitslücke, da im abgesicherten Modus viele Schutzsysteme umgangen werden können. Wir haben diesen Misstand an Microsoft gemeldet und warten derzeit auf eine Antwort. In der Zwischenzeit haben wir das Startverhalten im abgesicherten Modus so verändert,

dass WinSecure® auch beim Start im abgesicherten Modus gestartet wird. Wir arbeiten an einer Möglichkeit, bei Windows 2000 den Start im abgesicherten Modus zu verhindern und werden schnellstmöglich ein entsprechendes Servicepack zum Download anbieten.

10. Grundeinstellung des WinSecure® Filetreibers

Im Reiter „**Hilfe**“ befindet sich ein Button mit der Aufschrift „**Treiberabbild erstellen**“. Das Drücken des Buttons veranlasst WinSecure® dazu, ein Abbild des Filetreibers zu erstellen. Das angelegte Textfile wird auf **C:\Programme\Datapol\WinSecure PRO\Abbild.txt** geschrieben.

In diesem Textfile sieht man die Arbeitsvorschrift des Filetreibers. Es sind hier schon bestimmte Voreinstellungen vorhanden, die verhindern, dass ein Benutzer wichtige Daten des Betriebssystems verändert.



Die Syntax dieser Datei ist wie folgt gewählt:

Jede Zeile der Textdatei legt bestimmte Attribute für das in der Zeile spezifizierte Laufwerk, Verzeichnis oder die Datei fest.

In der zweiten Spalte (Spalten sind durch “|” getrennt) wird das Laufwerk angegeben. In unserem Beispiel steht in jeder Zeile ein Stern (*), was bedeutet, dass alle Laufwerke gemeint sind.

In der dritten Spalte sind dann Verzeichnisse und Dateien aufgeführt. Dabei können auch Wild-Cards vorkommen, die eine Menge von Dateien in einer Zeile spezifizieren.

Die vierte Spalte zeigt dann die jeweiligen Attribute, mit denen die Laufwerke, Verzeichnisse oder Dateien versehen sind. Diese sind im Einzelnen:

- *DelFi (Delete File): Das angegebene Verzeichnis oder die Datei darf nicht gelöscht werden.*
- *MkFi (Make File): Es darf auf dem angegebenen Laufwerk oder Verzeichnis kein gleichnamiges File erzeugt werden.*
- *OpFi (Open File): Ein angegebenes File darf nicht geöffnet werden.*
- *RenFi (Rename File): Die Datei darf nicht umbenannt werden.*
- *WrFi (Write File): Die Datei darf nicht überschrieben werden.*
- *RdFi (Read File): Die Datei darf nicht gelesen werden.*
- *ChAt (Change Attribute): Das Attribut des angegebenen Laufwerks, des Verzeichnisses oder der Datei darf nicht verändert werden.*
- *SubFo (Sub Folder): Es dürfen im angegebenen Verzeichnis keine Unterverzeichnisse angelegt werden.*
- *DenEx (Deny Execution): Die entsprechende Datei darf nicht ausgeführt werden.*
- *Hide (Hide): Das angegebene Laufwerk, Verzeichnis oder die angegebene Datei sind unsichtbar.*

11. Nutzungsbedingungen/ Lizenzvertrag

ENDBENUTZER-LIZENZVERTRAG FÜR SOFTWARE DER Datapol GMBH

WICHTIG - BITTE SORGFÄLTIG LESEN: Dieser Endbenutzer-Lizenzvertrag der Datapol GmbH ist ein rechtsgültiger Vertrag zwischen Ihnen (entweder als natürlicher oder juristischer Person) und der Datapol GmbH für das oben bezeichnete SPFTWAREPRODUKT der Datapol GmbH. Indem Sie das SOFTWAREPRODUKT installieren, erklären Sie sich einverstanden, durch die Bestimmungen dieses Lizenzvertrags gebunden zu sein. Falls Sie den Bestimmungen dieses Lizenzvertrags nicht zustimmen, sind Sie nicht berechtigt, das SOFTWAREPRODUKT zu installieren oder zu verwenden. Falls Sie das SOFTWAREPRODUKT erworben haben, können Sie es gegen volle Rückerstattung des Kaufpreises der Stelle zurückgeben, von der Sie es erworben haben.

Das SOFTWAREPRODUKT wird sowohl durch Urheberrechtsgesetze und internationale Urheberrechtsverträge geschützt als auch durch andere Gesetze und Vereinbarungen über geistiges Eigentum. Das SOFTWAREPRODUKT wird lizenziert, nicht verkauft.

1. LIZENZEINRÄUMUNG

Das SOFTWAREPRODUKT wird wie folgt lizenziert:

* Installieren und Verwenden: Datapol GmbH räumt Ihnen das Recht ein, Kopien des SOFTWAREPRODUKTS auf Ihren Computern, auf denen gültige lizenzierte Kopien desjenigen Betriebssystems ausgeführt werden, für das das SOFTWAREPRODUKT entwickelt wurde (z.B. Windows(r) 95, Windows NT, Windows 3.x, Macintosh usw.), zu installieren und zu verwenden. Falls mehrere Betriebssysteme auf ein und demselben Computer ausgeführt werden, benötigt der Lizenznehmer nur eine Lizenz.

* Sicherungskopien: Sie sind außerdem berechtigt, die für Sicherungs- und Archivierungszwecke notwendigen Kopien des SOFTWAREPRODUKTS anzufertigen.

2. BESCHREIBUNG WEITERER RECHTE UND EINSCHRÄNKUNGEN

Beibehaltung der Copyright-Vermerke: Sie sind nicht berechtigt, die Copyright-Vermerke auf den Kopien des SOFTWAREPRODUKTS zu entfernen oder zu ändern.

Vertrieb: Sie sind nicht berechtigt, Kopien des SOFTWAREPRODUKTS an Dritte weiterzuvertreiben.

Verbot im Hinblick auf Zurückentwicklung (Reverse Engineering), Dekompilierung und Disassemblierung: Sie sind nicht berechtigt, das SOFTWAREPRODUKT zurückzuentwickeln (Reverse Engineering), zu dekompilieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Beschränkung, dies ausdrücklich gestattet.

Vermietung: Sie sind nicht berechtigt, das SOFTWAREPRODUKT zu vermieten, zu verleasen oder zu verleihen.

Übertragung: Sie sind berechtigt, alle Ihre Rechte aus diesem Lizenzvertrag auf Dauer zu übertragen, vorausgesetzt, der Empfänger stimmt den Bestimmungen dieses Lizenzvertrags zu.

Supportleistungen: Die Datapol GmbH bietet Ihnen möglicherweise Supportleistungen in Verbindung mit dem SOFTWAREPRODUKT (“Supportleistungen”). Die Supportleistungen können entsprechend den Datapol GmbH-Bestimmungen und -Programmen, die im Benutzerhandbuch, der Dokumentation im Online-Format und/oder anderen von der Datapol GmbH zur Verfügung gestellten Materialien beschrieben sind, genutzt werden. Jeder ergänzende Softwarecode, der Ihnen als Teil der Supportleistungen zur Verfügung gestellt wird, wird als Bestandteil des SOFTWAREPRODUKTS betrachtet und unterliegt den Bestimmungen dieses Lizenzvertrags. Die Datapol GmbH ist berechtigt, die technischen Daten, die Sie der Datapol GmbH als Teil der Supportleistungen zur Verfügung stellen, für geschäftliche Zwecke, einschließlich der Produktunterstützung und -entwicklung, zu verwenden. Die Datapol GmbH verpflichtet sich, solche technischen Daten ausschließlich anonym im Sinne des Datenschutzes zu verwenden.

Beachtung aller anwendbarer Gesetze: Sie sind verpflichtet, das SOFTWAREPRODUKT nur in Übereinstimmung mit allen anwendbaren Gesetzen zu verwenden.

3. KÜNDIGUNG

Unbeschadet sonstiger Rechte ist die Datapol GmbH berechtigt, diesen Lizenzvertrag zu kündigen, sofern Sie gegen die Bestimmungen dieses Lizenzvertrags verstoßen. In einem solchen Fall sind Sie verpflichtet, sämtliche Kopien des SOFTWAREPRODUKTS zu vernichten.

4. EIGENTUM

Jegliche Eigentumsrechte, einschließlich, jedoch nicht beschränkt auf das Urheberrecht, an dem und in Bezug auf das SOFTWAREPRODUKT und jeder Kopie davon, liegen bei der Datapol GmbH oder deren Lieferanten. Eigentumsrechte und geistiges Eigentum am und in bezug auf den Inhalt, auf den durch das SOFTWAREPRODUKT zugegriffen wird, liegen beim jeweiligen Eigentümer und können durch entsprechende urheberrechtliche oder andere Gesetze über geistiges Eigentum geschützt sein. Dieser Lizenzvertrag gibt Ihnen keine Rechte an solchem Inhalt. Alle nicht ausdrücklich eingeräumten Rechte bleiben der Datapol GmbH vorbehalten.

5. GEWÄHRLEISTUNGSAUSSCHLUSS

Die Datapol GmbH schließt ausdrücklich jede Gewährleistung für das SOFTWAREPRODUKT aus. DAS SOFTWAREPRODUKT UND DIE DARAUF BEZOGENE DOKUMENTATION WIRD IHNEN “SO WIE SIE IST” ZUR VERFÜGUNG GESTELLT, OHNE GEWÄHR-

LEISTUNG IRGENDEINER ART, WEDER AUSDRÜCKLICH NOCH KONKLUDENT, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF KONKLUDENTE GEWÄHRLEISTUNGEN DER TAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DES NICHTBESTEHENS EINER RECHTSVERLETZUNG. DAS GESAMTE RISIKO, DAS AUS DEM VERWENDEN ODER DER LEISTUNG DES SOFTWAREPRODUKTS ENTSTEHT, VERBLEIBT BEI IHNEN.

6. BESCHRÄNKTE HAFTUNG

Bis zum durch anwendbares Recht äußerstenfalls Zulässigen können weder die Datapol GmbH noch deren Lieferanten haftbar gemacht werden für irgendwelche besonderen, zufällig entstandenen oder indirekten Schäden oder Folgeschäden (einschließlich, aber nicht beschränkt auf entgangenen Gewinn, Betriebsunterbrechung, Verlust geschäftlicher Informationen oder irgendeinen anderen Vermögensschaden), die aus dem Verwenden oder der Unmöglichkeit, das SOFTWAREPRODUKT zu verwenden, oder durch die Leistung bzw. Nichtleistung von Supportleistungen entstehen, und zwar auch dann, wenn die Datapol GmbH zuvor auf die Möglichkeit solcher Schäden hingewiesen worden ist. In jedem Fall bleibt die gesamte Haftung der Datapol GmbH auf den Betrag, den Sie für das SOFTWAREPRODUKT bezahlt haben, oder auf DM 10,- beschränkt, wobei der höhere Betrag maßgebend ist. Falls Sie jedoch mit der Datapol GmbH einen Vertrag über Supportleistungen abgeschlossen haben, wird die gesamte Haftung von der Datapol GmbH in Bezug auf Supportleistungen durch die Bestimmungen dieses Vertrags festgelegt. Da einige Staaten/Gerichtsbarkeiten den Ausschluss oder die Begrenzung der Haftung für Folge- oder zufällig entstandene Schäden nicht gestatten, gilt die vorstehende Einschränkung für Sie möglicherweise nicht.