Inhalt:

INHALT:		SEITE 1
Vorwort:		SEITE 1
HINTERGRUND:		SEITE 2
VORAUSSETZUNGEN:		SEITE 2
WAS IST WICHTIG:		SEITE 2
Vorgehensweise:		Seite 2
1.1 BACKUP:		SEITE 3
1.1.1	Systembackup	SEITE 3
1.2 DAS WIND	OWS BENUTZERKONTO VORBEREITEN:	SEITE 3
1.2.1	BENUTZERKONTO ANPASSEN:	SEITE 3
1.2.2	BENUTZERKONTO ÄNDERN:	SEITE 4
1.3 EXPORTIER	EN DES EFS-SCHLÜSSELS:	SEITE 5
1.3.1	EFS-SCHLÜSSEL EXPORT:	SEITE 5
1.4 SCAN2FIND	D-DATEIEN VERSCHLÜSSELN:	SEITE 11
1.4.1	DATEIEN VERSCHLÜSSELN:	SEITE 11
1.4.2	ANPASSUNGEN FÜR SCAN2FIND > 3.55:	SEITE 14
1.5 KONTROLLE	:	SEITE 15
1.5.1	ÜBER EXTERNES SYSTEM:	SEITE 15
1.5.2	ÜBER ANDERES BENUTZERKONTO:	SEITE 15
BESONDERHEITEN NTFS	zu Fat/Fat32:	SEITE 15
FAQ – HÄUFIGE FRAGEN	l	SEITE 15
BEGRIFFSERKLÄRUNG:		SEITE 17
EFS-SCHLÜSSEL IMPORT	IEREN:	SEITE 17

Vorwort:

Sollten Sie sich für die Windowseigene EFS Dateiverschlüsselung entscheiden, lesen sie bitte diese Anleitung KOMPLETT durch. Verschlüsseln sie die Dateien nur wenn Sie diese Anleitung komplett verstanden haben. Anderenfalls kommen Sie im schlimmsten Fall an Ihre eigenen Daten NIE mehr heran!

Hintergrund:

Alle in scan2Find hinterlegten Dokumente sind standardmäßig für alle einsehbar die im Besitz der Festplatte sind. Auch nach einer Formatierung der Festplatte sind diese Daten widerherstellbar. Um dies zu verhindern hilft die Windows-Bordeigene EFS Dateiverschlüsselung. Diese gilt nach wie vor als sicher. Bitte Beachten sie aber unbedingt den Abschnitt "Vorwort" da die reine Dateiverschlüsselung OHNE das Sichern des "Schlüssels" absolut riskant ist.

Voraussetzungen:

- 1.) Der Datenträger auf dem die Dateien von Scan2Find hinterlegt sind muss NTFS-Formatiert sein.
- 2.) Ein Betriebssystem ab Windows XP Prof. (Home wird nicht unterstützt)
- 3.) Das Windows Benutzerkonto muss mit einem Passwort versehen sein und der Option "Ja, nur für eigene Verwendung"

Was ist wichtig:

Je nach Einsatz von Scan2Find kann es mehr oder weniger wichtig sein, die in Scan2Find hinterlegten Dateien vor dem Zugriff unbefugter Personen zu sichern.

Scan2Find leistet hier schon eine gute Vorarbeit indem alle Dateien die hinterlegt werden "einfach" durchnummeriert werden sodass allein aus dem Dateinamen keine Rückschlüsse auf den Inhalt der Datei zu schließen sind. So kann beispielsweise ein unbefugter Nutzer mit der Datei 0016.S2F keine Rückschlüsse auf den Inhalt der Datei schließen. Anders wäre es bei einer Datei mit dem Namen Müller_Abmahnung.S2F oder Rechtstreit_Müller_gegen_Fischer.S2F. Hier kann ein unbefugter Nutzer schon Rückschlüsse ziehen dass Beispielsweise die Frau/Herr Müller eine Abmahnung erhalten hat bzw. die Frau/Herr Müller im Rechtstreit mit dem der Frau/Herrn Fleischer liegt. Den Part der verräterischen Dateinamen können wir also unberücksichtigt lassen wenn es um die Dateiverschlüsselung von Scan2Find Dateien geht.

Anders sieht es mit den Dateien selbst aus. Die bloße Endung *.S2F bietet wenig Schutz. Mit einem Doppelklick auf eine *.S2F-Datei wird mir Windows zwar die Meldung bringen dass es keine Verknüpfung zu diesem Dateityp gibt, wähle ich aber beispielsweise das Windows-Bordeigene Programm Paint für das öffnen und anschauen von *.S2F-Dateien aus so wird mir in Paint letztlich die Datei dargestellt. Genau hier soll nun die EFS-Dateiverschlüsselung ansetzen und dies nur noch für ausgewählte Benutzer erlauben.

Vorgehensweise:

- 1.1 Als erstes machen wir ein Backup ALLER wichtigen Dateien auf dem Computer. Dabei ist es unerheblich ob es sich um Scan2Find-eigene Dateien handelt oder über die "Eigenen Dateien" als solches.
- 1.2 Wir vergewissern uns dass das Windows Benutzerkonto mit einem Passwort und der Option "Ja, nur für eigene Verwendung" versehen ist.
- 1.3 Wir exportieren den EFS-Schlüssel auf ein Externes sicheres Speichermedium (Keine Diskette, CD oder DVD! Hier eignen sich am besten Speichersticks oder Speicherkarten)
- 1.4 Wir verschlüsseln alle Scan2Find Dateien und nehmen noch einige Anpassungen vor.
- 1.5 Kontrolle der verschlüsselung

1.1 Das Backup

1.1.1 Da von der EFS-Verschlüsselung nicht nur die in Scan2Find hinterlegten Dateien verschlüsselt werden können und eventuell von Windows standardmäßig schon einige Dateien nach aktivierter Verschlüsselung verschlüsselt werden ist es wichtig alle Dateien vorher zu sichern bzw. ein Backup des Systems zu erstellen.

1.2 Das Windows Benutzerkonto vorbereiten

1.2.1 Unter *Start->Systemsteuerung->Benutzerkonten* können wir ein Kennwort für den Windows Benutzer einstellen.

Ist dies noch nicht geschehen wird Windows die Frage stellen: **"Möchten Sie Ihre Dateien und Ordner nur für die eigene Verwendung einschränken?"**. Hier müssen wir die Option: **"Ja, nur für eigene Verwendung."** aktiviren. Wenn dies der Fall ist lesen sie bitte ab Punt 1.3.1 weiter.



1.2.2 Ist schon ein Kennwort erstellt so löschen Sie bitte das Kennwort



Und erstellen nun ein neues Kennwort wie im Abschnitt 1.2.1

1.3 Exportieren des EFS-Schlüssels

1.3.1 Um nun den EFS-Schlüssel zu exportieren öffnen Sie dazu den Internetexplorer und klicken hier auf *Extras->Internetoptionen*. Wechseln Sie hier zum Kartenreiter Inhalte:

Internetoption	en				? ×
Verbind	lungen	Pro	gramme		Erweitert
Allgemein	Sic	therheit	Datensch	nutz	Inhalte
Inhaltsratge	ber Filter helfen I diesem Compl	hnen bei der I uter angezeig A <u>k</u> tivi	Kontrolle der I t werden könr eren	nternetin nen. Einst	ihalte, die auf :ellungen
Zertifikate					
	Zertifikate we Identifizierun(erden für vers g verwendet.	chlüsselte Ver	bindunge	en und zur
<u>S</u> SL-St	atus löschen:	<u>Z</u> ert	ifikate	Hera	usgeber
AutoVervolls	ständigen – AutoVervollst vorherige Eing und schlägt Ü	ändigen speic gaben auf We Ibereinstimmu	hert ebseiten ngen vor.	Einst	ellungen
k	Feeds bieten Websites, die anderen Prog önnen.	aktualisierte I ∶in Internet E rammen geles	inhalte von (xplorer und en werden	Ei <u>n</u> st	ellungen
		0	< Abl	orechen	Übernehmen

Wählen sie in der Mitte den Button Zertifikate aus. Es wird sich folgendes Fenster öffnen:

Anleitung zur Windows EFS Dateiverschlüsselung auf NTFS-Datenträgern

Zertifikate				2	x
<u>B</u> eabsichtigter	<alle></alle>				•
Eigene Zertifikate	Andere Personen	Zwischenzertifiz	ierungsstellen	Vertrauenswürdige :	×
Ausgestellt für	Ausgeste	ellt von	Gültig bis	Angezeigter Name	
Thomas	Thomas		01.05.2107	<kein></kein>	
Importieren Ex Beabsichtigte Zwee	portieren) <u>E</u> nt :ke des Zertifikats	fernen		Erweitert.	
Verschlusseindes	Dateisystem			Anzeigen	
				<u>S</u> chließer	n

Aktiviren sie nun durch anklicken das entsprechende Benutzerkonto dessen EFS-Schlüssel exportiert werden soll. Das entsprechende Zertifikat ist immer 100 Jahre gültig und wird unter "Beabsichtigte Zwecke des Zertifikats" als "Verschlüsseltes Dateisystem" angezeigt. Klicken Sie hier nun auf *Exportieren* und folgend sie dem Assistenten:



Wahlen Sie im nachfolgendem Dialog "Ja, privaten Schlüssel exportieren" aus und klicken sie auf *Weiter*

Zertifikatsexport-Assistent
Privaten Schlüssel exportieren Sie können den privaten Schlüssel mit dem Zertifikat exportieren.
Private Schlüssel sind kennwortgeschützt. Wenn Sie den privaten Schlüssel mit dem ausgewählten Zertifikat exportieren möchten, müssen Sie auf einer der folgenden Seiten ein Kennwort eingeben.
Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?
Da, privaten Schlüssel exportieren
🔘 <u>N</u> ein, privaten Schlüssel nicht exportieren
< <u>Z</u> urück <u>W</u> eiter > Abbrechen

Im nun folgendem Dialog stellen Sie bitte alles wie es im nachfolgendem Bild zu sehen ist ein und klicken anschließend auf *Weiter*

Exportdateiformat Zertifikate können in verschiedenen Dat	eiformaten exportiert werden.
Wählen Sie das gewünschte Format:	
C DER-codiert-binär X,509 (,CER)	
C Base-64-codiert X.509 (.CER)	
C Syntaxstandard kryptografische	r Meldungen - "PKCS #7"-Zertifikate (.P7B)
🔲 We <u>n</u> n möglich, alle Zertifikati	e im Zertifizierungspfad einbeziehen
Privater Informationsaustausch	- PKCS #12 (.PFX)
🔲 W <u>e</u> nn möglich, alle Zertifikati	e im Zertifizierungspfad einbeziehen
🔽 <u>V</u> erstärkte Sicherheit aktivier	en (IE 5.0, NT 4.0 SP4 oder höher erforderlich)
Privaten Schlüssel nach erfol	greichem Export löschen
	< <u>Z</u> urück <u>W</u> eiter > Abbrechen

Im nun folgendem Dialog vergeben Sie bitte ein Kennwort. Das Kennwort muss NICHT dem Benutzerkennwort entsprechen. Sie sollten sich aber dieses Kennwort gut merken denn ohne dieses Kennwort können Sie im Notfall den exportierten EFS-Schlüssel nicht nutzen. Klicken Sie auch hier nun wieder auf den Button *Weiter*:

	wort
De Sie	er private Schlüssel muss mit einem Kennwort geschützt werden, um die cherheit zu gewährleisten.
-	
Ge	eben Sie ein Kennwort ein und bestätigen Sie dieses.
	Kennwort:

	Kennwort bestätigen:

	J

Speichern unter						? ×
Spe <u>i</u> chern in:	🛯 🔒 EFS-Schlüsse	el_Thomas	•	6	۰ 对 🌶	
Zuletzt verwendete D						
Desktop						
è Eigene Dateien						
Arbeitsplatz						
	Datei <u>n</u> ame:	EFS_Schlüssel_	Thomas		•	<u>S</u> peichern
Netzwerkumgeb	Datei <u>t</u> yp:	Privater Informa	tionsaustausch (*.pf	x)	•	Abbrechen

Klicken Sie auf Durchsuchen und speichern sie den EFS-Schlüssel auf einem Externem Speichermedium ab:

ertifikatsexport-Assistent				x
Exportdatei Geben Sie die den Namen o	ler zu exporti	erenden Datei ar	n.	
D <u>a</u> teiname:				
I:\EFS-Schlüssel_Thomas\E	FS_Schlüssel_	Thomas.pfx	Durchsuchen	
		< <u>Z</u> urück	Weiter > Abbrech	en

Ihnen wird nun noch einmal die Zusammenfassung des Exports angezeigt. Klicken Sie hier auf *Fertig stellen*.



Ist der Vorgang erfolgreich beendet wird Ihnen dies mit einer entsprechenden Meldung Quittiert.

Zertifikatsexport-Assistent
Der Exportvorgang wurde erfolgreich abgeschlossen.
ОК

- 1.4 Scan2Find-dateien verschlüsseln
- 1.4.1 Klicken sie auf den Arbeitsplatz und wechseln Sie in das Verzeichnis wo sich der Scan2Find-Ordner mit allen Dokumenten befindet. In meinem Fall ist das der Speicherort: D:\Eigene Dateien wo sich der Ordner \scan2find befindet. Klicken sie mit der rechten Maustaste den Ordner scan2find an und gehen sie in dem sich öffnendem Kontextmenü auf den Menüpunkt *Eigenschaften*. Sie erhalten folgende Ansicht:

Eigenschaften v	on scan2find
Allgemein Frei	igabe Anpassen
	scan2find
Тур:	Dateiordner
Ort:	D:\Eigene Dateien
Größe:	2,36 GB (2.544.135.303 Bytes)
Größe auf Datenträger:	2,37 GB (2.554.171.392 Bytes)
Inhalt:	4.450 Dateien, 134 Ordner
Erstellt:	Donnerstag, 25. August 2005, 17:57:29
Attribute:	■ <u>Schreibgeschützt</u> <u>V</u> ersteckt
	OK Abbrechen Übernehmen

Klicken sie nun auf den Button Erweitert und aktivieren sie die Kästchen wie im Nachfolgendem Bild:

Enweiterte Attribute
Wählen Sie die Einstellungen für diesen Ordner. Wenn Sie die Änderungen übernehmen, können Sie angeben, ob die Änderungen auch auf Unterordner und Dateien angewendet werden sollen.
 Ordner kann archiviert werden Inhalt f ür schnelle Dateisuche indizieren
Komprimierungs- und Verschlüsselungsattribute Inhalt <u>k</u> omprimieren, um Speicherplatz zu sparen Inhalt <u>v</u> erschlüsseln, um Daten zu schützen Details
OK Abbrechen

Mit einem Klick auf *OK* wird sich dieses Fenster wieder schließen und Sie gelangen wieder zu folgender Ansicht:

Eigenschaften vo	on scan2find
Allgemein Frei	gabe Anpassen
	scan2find
Тур:	Dateiordner
Ort:	D:\Eigene Dateien
Größe:	2,36 GB (2.544.135.303 Bytes)
Größe auf Datenträger:	2,37 GB (2.554.171.392 Bytes)
Inhalt:	4.450 Dateien, 134 Ordner
Erstellt:	Donnerstag, 25. August 2005, 17:57:29
Attribute:	<u>S</u> chreibgeschützt <u>Erweitert</u>
	OK Abbrechen Ü <u>b</u> ernehmen

Wenn Sie nun auf den Button Übernehmen klicken, wird Ihnen der Nachfolgende dialog angezeigt:

Änderungen der Attribute bestätigen	
Die folgenden Attributänderungen werden durchgeführt:	
Verschlüsseln	
Soll die Änderung nur für diesen Ordner oder auch für alle Unterordner und Dateien übernommen werden?	
🔘 Änderungen nur für diesen Ordner übernehmen	
Anderungen für diesen Ordner, Unterordner und Dateien übernehmen	
OK Abbrechen	

Aktivieren sie die Option **"Änderungen für diesen Ordner, Unterordner und Dateien übernehmen**" und klicken Sie anschließend den Button OK. Windows wird nun anfangen alle Dateien zu verschlüsseln. Bitte beachten Sie dass dieser Vorgang einige zeit in Anspruch nehmen kann.

Ist dieser Vorgang abgeschlossen wird der Ordner scan2find sowie alle Unterverzeichnisse nicht mehr in schwarz sondern in grün dargestellt. (Standard-Windowskonfiguration) Die grüne Ordner und Dateifarbe ist ein Zeichen für verschlüsselte EFS-Dateien. Alle diese Ordner

und Dateien können von nun an lediglich von dem Benutzer geöffnet werden der diese Dateien erstellt hat. Andere Nutzer können diese Dateien nur öffnen wenn der Exportierte EFS-Schlüssel in das System importiert wurde.

1.4.2 Folgende Anpassungen müssen in der Scan2find Ordnerverschlüsselung vorgenommen sofern Sie Scan2Find bis Version 3.55 einsetzen. Wechseln Sie in den Ordner D:\xyz\scan2find\s2fInternDat\admin (Der Pfad wird auf Ihrem System abweichen) und klicken Sie mit der rechten Maustaste auf den Ordner Mails und im nun folgendem Kontextmenü auf den Menüpunkt *Eigenschaften*.

Eigenschaften von Mails		
Allgemein Frei	igabe Anpassen	
	Mails	
Тур:	Dateiordner	
Ort:	D:\Eigene Dateien\scan2find\s2fInternDat\admin	
Größe:	36,7 MB (38.581.983 Bytes)	
Größe auf Datenträger:	40,0 MB (42.041.344 Bytes)	
Inhalt:	1.176 Dateien, 5 Ordner	
Erstellt:	Donnerstag, 1. Februar 2007, 20:31:45	
Attribute:	Schreibgeschützt	
	OK Abbrechen Obernehmen	

Klicken sie nun auf den Button *Erweitert* und aktivieren Sie Kästchen wie im nachfolgendem Bild:

Enweiterte Attribute	? ×	
Wählen Sie die Einstellu Wenn Sie die Änderung die Änderungen auch a werden sollen.	ngen für diesen Ordner. Ien übernehmen, können Sie angeben, ob uf Unterordner und Dateien angewendet	
Archiv- und Indexattribute	den :he indizieren	
Komprimierungs- und Verschlüsselungsattribute		
	OK Abbrechen	

Klicken sie nun auf *OK* und im nachfolgendem Dialog auf *Übernehmen*. Dies ist notwendig da sonst die Mails in Scan2Find nicht mehr angezeigt werden. Ab der Version 3.5X ist dieser Schritt nicht mehr notwendig da ab dieser Version alle Mails in einer gesonderten Datenbank hinterlegt werden.

- 1.5 Kontorolle
- 1.5.1 Um nun zu kontrollieren ob unsere Verschlüsselung Erfolg hatte, gibt es verschiedene Möglichkeiten. Kopieren sie eine verschlüsselte Datei dazu einfach auf einen NTFs-Formatierten Datenträger und versuchen Sie diese Datei auf einem anderem PC zu öffnen. Die Datei sollte sich nun zwar öffnen lassen, der Inhalt jedoch wird aus völlig wirren Zeichen bestehen. Ohne dass der erforderliche EFS-Schlüssel in dieses System importiert wird, gibt es keine Möglichkeit diese Datei zu betrachten.
- 1.5.2 Eine Weitere Möglichkeit besteht darin, sich auf dem Rechner auf dem sich Scan2Find befindet unter einem anderem Konto anzumelden und zu versuchen eine verschlüsselte Datei zu betrachten. Auch hier wird zwar die Anzeige erlaubt, der Inhalt jedoch wird wieder aus wirren Zeichen bestehen und somit unbrauchbar sein.

Besonderheit NTFS zu FAT/FAT32

Eine Besonderheit stellt das kopieren einer verschlüsselten Datei von einem NTFS-Datenträger auf einen FAT oder FAT32 formatierten Datenträger dar.

FAQ – Häufige Fragen

Frage:	Wie Sicher ist diese Art der Verschlüsselung?
Antwort:	Die Verschlüsslung von Daten über die EFS-Dateiverschlüsselung gilt nach wie vor als "ungeknackt" und Sicher.
Frage: Antwort:	Kann mein Administrator meine über EFS-Verschlüsselten Dateien anschauen? Keiner,- auch nicht der Administrator des Computers ist in der Lage die via EFS verschlüsselten Dateien eines Nutzers anzuschauen.

Anleitung zur Windows EFS Dateiverschlüsselung auf NTFS-Datenträgern

Frage:	Wenn der Administrator mein Benutzerkennwort ändert und sich auf meinem Account einloggt, hat er dann Zugriff auf meine mit FES-Verschlüsselten Dateien?
Antwort:	Nein! Nur Kennwortänderungen die Sie als Benutzer selbst durchführen berechtigen zum Lesen dieser Dateien! Ändert ein anderer Nutzer außer Sie selbst das Kennwort ist kein Zugriff auf diese Dateien möglich!
Frage:	kann ich mit Hilfe eines anderen Betriebssystems wie zum Beispiel Linux die mit EFS- verschlüsselten Dateien anzeigen lassen?
Antwort:	NEIN!
Frage:	Gibt es ein Programm mit dessen Hilfe ich EFS-Verschlüsselte Dateien "Knacken" kann?
Antwort:	NEIN!
Frage:	ich habe mein Passwort vergessen und der Administrator hat mein Passwort zurückgesetzt. Nun komme ich nicht mehr an meine EFS-verschlüsselten Daten. Was kann ich tun?
Antwort:	Sich an das alte Passwort erinnern oder den gesicherten Schlüssel/Zertifikat in das System wieder importieren.
Frage:	Welche Betriebssysteme bieten diese EFS-Verschlüsselung?
Antwort:	EFS ist ab Windows 2000 im System integriert ausgenommen Windows XP Home.
Frage: Antwort:	Ist die EFS-Verschlüsselung von Windows 2000 genau so sicher wie bei XP? Nein! Bei Windows 2000 setzt sich der Schlüssel für EFS lediglich aus dem Benutzernamen und dem Passwort des Users zusammen. Dies hat den Nachteil dass alle User in einem Netzwerk die über den gleichen Benutzernamen mit gleichem Passwort verfügten die Dateien entschlüsseln und somit anschauen konnten. Ab Windows XP wird stattdessen die SID zu Verschlüsselung herangezogen.
Frage: Antwort:	Werden bei einem Backup meine mit EFS-Verschlüsselten Daten mit gesichert? Alle aktuellen Backupprogramme sind in der Lage EFS-Dateien zu sichern.
Frage:	Kann ich mir EFS-verschlüsselte Daten aus einem Backup anschauen ohne den
Antwort:	Nein! Wie der Name schon sagt – es handelt sich hier lediglich um ein Backup. Ein Backupprogramm bietet KEINE Entschlüsselung an!
Frage:	Ich habe mein System neu Installiert und den gleichen Benutzer mit gleichem Passwort wieder erstellt. Trotz dem kann ich meine Dateien nicht lesen?
Antwort:	Einen Identischen Benutzer zu erstellen reicht aus. Wichtiger ist der Import des gesicherten EFS-Schlüssels! Ist dieser nicht vorhanden sind die Daten unwiderruflich unbrauchbar!
Frage: Antwort:	Wie erreiche ich das Maximum an Sicherheit bei der EFS-Verschlüsselung? Als erstes sollte ein starkes Passwort benutzt werden. Sämtliche alten Backups sollten vernichtet werden da dort die Daten noch unverschlüsselt vorliegen. Weiterhin ist es ratsam den Recovery-Agent zu deaktivieren.
Frage:	Wer haftet bei Verlust des EFS-Schlüssels und wen kann ich verklagen wenn es schief geht.

Anleitung zur Windows EFS Dateiverschlüsselung auf NTFS-Datenträgern

- Antwort: Sie selbst! Sie haften für alle Schritte die Sie unternehmen. Diese Anleitung dient lediglich als kleine Hilfe bei der Verschlüsselung der Daten von Scan2Find. An dieser Stelle bitte ich noch einmal darum diese Anleitung erst komplett zu lesen und gegebenenfalls weiter im Internet zu Recherchieren bevor Sie die EFS-Dateiverschlüsselung ihres Systems Aktiviren.
- Frage: Kann ich die Dateien Verschlüsseln und gleichzeitig die Option "Komprimieren" anwenden?
- Antwort: Nein, dass ist nicht möglich. Wenn Sie sich für die Dateiverschlüsselung entscheiden haben können Sie die Dateien nicht zusätzlich Komprimieren.

EFS-Schlüssel Importieren

Um den EFS-Schlüssel zu importieren genügt ein Doppelkick auf den Exportierten Schlüssel. Es folgt ein kleiner Assistent der Sie durch den Importvorgang führt.

Begriffserklärung:

- NTFS: New Technology File System
- FAT: File Allocation Table (Dateizuordnungstabelle)
- EFS: Encrypted File System (Dateiverschlüsselung auf NTFS-Datenträgern)
- SID: Security Identifeir (Identifikationsnummer)

Verantwortlich für diese Anleitung ist:

Thomas Reichel Postfach 1332 23833 Bad Oldesloe

Fon: 040-30033187 Mail: info@nordigspace.de