

## Windows NT – Handbuch für Betriebsräte

Windows NT : Handbuch für Betriebsräte

Regelungsbedarf und Kontrollmöglichkeiten

Michael Kürschner ; Helmut Teppich– Düsseldorf : Hans-Böckler-Stiftung, 1999

ISBN 3-928204-92-0



### ■ Beschreibung

Wo und wie unterliegt die Anwendung von Windows NT der Information, Beratung und/oder der Mitbestimmung. Wie kann bei der Wahrnehmung der Arbeitnehmer-Rechte vorgegangen werden? Dieses Buch liefert Unterstützung für Betriebs- und Personalräte.

## ■ Einleitung

Die Idee zu diesem Buch entstand im Rahmen verschiedener Beratungen, bei denen Windows NT direkt oder indirekt Thema zwischen Betriebs- bzw. Personalräten und Geschäftsleitungen war. Auf Seiten der Interessenvertretungen (oft aber auch auf Seiten der Geschäftsleitungen) lagen keine bzw. nur sehr begrenzte Kenntnisse vor, wo und wie die Anwendung von Windows NT der Information, Beratung und/oder der Mitbestimmung unterliegt und vor allem, wie bei der Wahrnehmung dieser Rechte vorgegangen werden könnte. Bei dem Versuch, "das Rad nicht neu zu erfinden" und auf andere Erfahrungen bzw. Regelungen zurückzugreifen, stellte sich aber unter anderem heraus, dass es zwar eine Reihe guter deutscher Quellen zu den Themen NT-Sicherheit bzw. NT-Benutzerverwaltung gibt, die Sichtweise auf Windows NT aus dem Blickwinkel der Beschäftigten bzw. ihrer Interessenvertretungen aber kein Gegenstand in den Veröffentlichungen ist. Datenschutz, Kontrolle von Leistung und Verhalten sowie das Betriebsverfassungsgesetz sind dort keine Stichworte.

Ziel dieser Veröffentlichung ist es, Betriebs- und Personalräte zu unterstützen und ihre Beteiligungsrechte möglichst kompetent wahrzunehmen. Dazu haben wir unsere Beratungserfahrungen bei Anwendung von Windows NT Version 4 genutzt. Es werden die nach unserer Erfahrung relevanten Aspekte der Anwendung von Windows NT dargestellt und – soweit möglich – anhand von Bildschirmanzeigen erläutert. Diese Art der Darstellung soll/kann z.B. bei Begehungen oder Prüfungen von NT-Systemen als Unterstützung und Referenz verwendet werden..

Bei der Darstellung und den Lösungsvorschlägen haben wir uns auf die NT-eigenen "Bordmittel" beschränkt, wodurch auch das Arbeitgeberargument : "Das kostet zusätzliches Geld." umgangen wird, obwohl eine gute Sicherheitsstrategie auch Zeit und damit Geld kostet.

Vor dem Hintergrund dieses Ansatzes kann und will dieses Buch in keinem Fall einen Anspruch auf Vollständigkeit erheben, zumal Windows NT ein komplexes Produkt ist und der Wald vor lauter Bäumen manchmal nicht sichtbar wird. Viele, für DV-kundige Betriebs- und Personalräte, unter Umständen interessante Vertiefungen und Details sind auch deshalb unberücksichtigt geblieben, um diese Veröffentlichung in einem vertretbaren Umfang zu halten. Themen, die aus unserer Sicht für die Wahrnehmung der Aufgaben des Betriebs- oder Personalrats bei der Regelung von Windows NT nicht zwingend notwendig sind, bleiben deshalb unberührt.

Spezielle Server-Versionen wie die Small Business Server (SBS)- und die Enterprise-Version oder der Terminal-Server werden deshalb nur erwähnt, ebenso wurden Fragestellungen zu NT-basierten Anwendungen oder den verschiedenen Back Office-Programmen (Exchange, SQL Server, SMS, IIS) nicht behandelt. Zur Vertiefung dieser Details wird auf die Quellen im Anhang verwiesen.

Zur Erstellung dieses Buches wurden Pentium-Rechner mit NT Workstation 4/Servicepack3 (Build 1381) und NT Server 4/Servicepack3 (Build 1381) eingesetzt.

## ■ Inhaltsverzeichnis

---

1. Einleitung
  - 1.1 Vorwort
  - 1.2 Überblick
2. Windows NT – Das Konzept
  - 2.1 Entwicklung von Windows NT
  - 2.2 Systemtypen
  - 2.3 Organisationskonzepte
    - 2.3.1 Das Arbeitsgruppenkonzept
    - 2.3.2 Das Domänenkonzept
  - 2.4 Benutzer- und Gruppenverwaltung
    - 2.4.1 Benutzerverwaltung
    - 2.4.2 Benutzerverwaltung mit Befehlseingabe
    - 2.4.3 Gruppen
    - 2.4.4 Globale Gruppen
  - 2.5 Weitere wichtige Funktionen im Benutzermanager
    - 2.5.1 Richtlinien für Konten
    - 2.5.2 Richtlinien für Benutzerrechte
    - 2.5.3 Überwachungsrichtlinien
  - 2.6 Freigaben
  - 2.7 NTFS und Zugriffsrechte
  - 2.8 Registry
  - 2.9 RAS ( Remote Access Service)
3. Sicherheit – Einrichten und Überwachen
  - 3.1 Sicherheitsmerkmale von Windows NT (unvollständige Auflistung)
  - 3.2 C2 Zertifizierung
  - 3.3 Systemrichtlinien
  - 3.4 Benutzerprofile
  - 3.5 Überwachung und Kontrolle
    - 3.5.1 Überwachung einstellen
    - 3.5.2 Überwachung prüfen mit der Ereignisanzeige
    - 3.5.3 Dateien der Ereignisanzeige
    - 3.5.4 Zeichen der Ereignisanzeige
    - 3.5.5 Beispiele für Meldungen der Ereignisanzeige
    - 3.5.6 Meldungen der Ereignisanzeige (EventLog)
    - 3.5.7 NT-eigene Werkzeuge zur Informationssammlung
4. Umsetzung der Datenschutzrichtlinien-Vorgaben des § 9 BDSG
5. Windows NT – Eine mitbestimmungspflichtige technische Einrichtung
6. Windows NT 5 bis Windows 2000
7. Nützliche Programme zur Begehung, Kontrolle und Administration von Windows NT
  - 7.1 ELWIZ (EventLog Wizard) 1.35
  - 7.2 DumpACL (v2.716)
  - 7.3 EventList – Zusammenfassung von Eventdateien, Version 2.8
  - 7.4 Sicherheitsmanager 1.1 für Windows NT 4.0
  - 7.5 Visual Netinfo Preview 2
  - 7.6 Security Configuration Wizard NT 2b
8. Begehung eines Windows-NT-Systems
  - 8.1 Dokumentation der Begehung

- 8.2 Voraussetzungen für eine Begehung
- 8.3 Beispiel : Checkliste für die Begehung eines Windows NT-Systems /-Domäne
- 8.4 Domänenorganisation
- 8.5 Administration und Benutzerverwaltung
- 8.6 Richtlinien
- 8.7 Überwachung
- 8.8 Personenbezogene Daten
- 8.9 Ereignisanzeige
- 8.10 Kontrolle der aktuellen und gespeicherten Ereignisanzeige des PDC/des lokalen Rechners nach Fehlercodes
- 8.11 RAS
- 8.12 Installierte Software/Zusatzsoftware
- 8.13 Hinweise zur Checkliste
- 9. Beispiel für eine Windows-NT-Vereinbarung
- 10. Quellenverzeichnis
  - 10.1 Literatur (deutsch)
  - 10.2 Literatur (englisch)
  - 10.3 Internet Ressourcen (deutsch)
  - 10.4 Internet Ressourcen (englisch)
  - 10.5 Electronic Newsletters (deutsch)
  - 10.6 Electronic Newsletters (englisch)
  - 10.7 Windows NT Shareware (deutsch)
  - 10.8 Windows NT Tools (englisch)
- 11. Schlagwortverzeichnis
- 12. Abbildungsverzeichnis

## ■ Leseprobe

### ***Begehung eines Windows NT Systems***

Begehungen von EDV-Systemen sind nach unserer Erfahrung immer dann unverzichtbar, wenn viele Details nur durch genaues Ansehen sinnvoll zu begreifen sind. Wer Begehungen oder Vorführungen von DV-Systemen bereits mitgemacht hat, kennt die Situation, daß sich aus einer Frage eine weitere ergibt. Diese führt zu wieder einer anderen und schließlich steht man in einem Thema, das so vorher gar nicht vorbereitet wurde, weil die Bedeutung bei den vorhergehenden Verhandlungen/Gesprächen oder der vorbereitenden Sichtung von Unterlagen nicht erkennbar war.

Eine andere Erfahrung ist die, das vieles, was bei der Begehung geprüft wurde, untergeht, weil es vergessen wurde. Dies liegt oft daran, daß keine genügende Vorbereitung stattfand und/oder das keine Prüfliste vorbereitet wurde, an der sich alle Beteiligten bei der Begehung „entlanghangeln“ können. Die Gefahr, etwas von dem, was vorbereitet wurde, zu vergessen, ist bei dieser Vorgehensweise gering.

### ***Dokumentation der Begehung***

Mitschreiben, insbesondere von Bildern, ist in der Kürze der Begehungszeit oft nicht möglich. Für die weitere Sichtung und Beurteilung der dabei gewonnenen Erkenntnisse durch die Interessenvertretung, die ja nicht am NT-Arbeitsplatz stattfindet, ist es hilfreich und notwendig, wenn die gesehenen Bilder dann auch zur Verfügung stehen.

Da inzwischen fast auf jedem Windows-Rechner Word installiert ist, kann man folgendermaßen vorgehen: Das Programm Word bleibt während der gesamten Begehung offen (im Hintergrund). Jedesmal, wenn auf dem Bildschirm etwas interessantes auftaucht, wird per Tastendruck ALT + „Taste Druck“ ein Bildschirm „photo“ erzeugt. Wechsel zu Word ist möglich mit den Tasten „Alt + Tab“. Das zwischengespeicherte Bild ist mit STRG + V in die geöffnete leere Datei einzusetzen.

Es wird empfohlen, die Datei nach jedem Einsatzvorgang abzuspeichern. Am Ende der Begehung ist unter Umständen eine dicke Datei (mit mehreren MB) vor. Nach Beendigung der Begehung sollte die Datei sofort komplett ausgedruckt werden. Sofern möglich, sollte sie - für spätere Prüfungen - zusätzlich auf den Betriebsratsrechner oder -server gespeichert werden.

### ***Voraussetzungen für eine Begehung***

Begehungen sollten direkt am PDC, mindestens aber an einem Administratorarbeitsplatz stattfinden. Es muß vorher verabredet sein, daß die Person, die das System vorführt, höchste Rechte am System hat, also Domänenadministrators und Administrator des lokalen Rechners ist. Andernfalls kommt es nicht selten zu Situationen, in denen der anwesende Administrator nicht „weiter kann“. Die weitere Begehung ist dann eigentlich zwecklos.

Falls die Begehung an einem Administratorarbeitsplatz stattfindet, sollte anschließend aber auch der PDC und stichprobenartig ein oder zwei BDCs vor Ort begangen werden. Bei der Begehung der Server sollte auch die Aufbewahrung der Sicherungsmedien geprüft werden. Zugriff und Schutz müssen denen der Server entsprechen.

Als hilfreich hat sich die Mitnahme von eigenen Hilfsprogrammen erwiesen. Dies erfordert natürlich eine Abstimmung mit dem Arbeitgeber und den Administratoren und vor allem Erfahrung mit dem Programm selbst. Die vorgestellten Programme passen jedes für sich auf eine normale Diskette. Sofern die Möglichkeit besteht, ist das Erstellen einer eigenen Prüf-CD mit verschiedenen Programmen, z.B. aus dem Windows NT Ressource Kit (Technische Referenz), sinnvoll.

**Beispiel : Checkliste für die Begehung eines Windows NT - Systems/-Domäne**

Die folgende Checkliste ist wie jede Checkliste - nur soweit sinnvoll, wie sie an die betrieblichen Gegebenheiten angepaßt wird. Dazu haben wir die unseres Erachtens relevanten Fragen für das Erkennen und gegebenenfalls Bewerten von Beteiligungstatbeständen zusammengestellt.

**Domänenorganisation**

1. Wie heißt die Domäne?

---

2. Zu welchem Typ gehört der Rechner, über den der Zugriff bei der Begehung erfolgt?

Primärer Domänen-Controller (PDC)

Sicherungs-Domänen-Controller (BDC)

Server

Workstation

3. Wie heißt der Primäre Domänen-Controller der Domäne (Name / IP Nummer)

---

4. Gibt es weitere Domänen ? Wenn ja, welche ?

---

5. Gibt es bei dem Einsatz mehrerer Domänen-Server Vertrauensstellungen (Trusts) zwischen diesen Rechten?

Ja

Nein

Teilweise

6. Welche Art von Vertrauensstellung besteht zwischen welchen Domänen-Servern?

Einseitige Vertrauensstellungen

von

nach

Gegenseitige Vertrauensstellungen

von

zu

7. Gibt es versteckte Server, Workstations oder Drucker in der Domäne? Welche ?

---

8. Welche Rechner in der Domäne sind nicht komplette NTFS formatiert ? Welches zusätzliche Betriebssystem?

---

**Administration und Benutzerverwaltung**

9. An welche Personen ist das Konto Domänen-Administrator vergeben oder ist es „gesperrt“?

---

10. Ist das Konto Administrator an eine oder mehrere Personen vergeben oder gesperrt?

---

11. Werden die Konten der Sub-Administratoren in der Domäne verwendet? Welche? Wer ist Mitglied?

Sub-Administrator

Name des Mitglieds

12. Werden die Konten der Sub-Administratoren auf den anderen Servern und Workstations verwendet? Welche? Wer ist Mitglied?

---

13. Welche Administratoren haben zusätzlich normale Benutzerkonten?

---

Funktion Admin	Benutzername

14. Welche globalen und lokalen Gruppen in der Domäne gibt es zusätzlich neben den Systemgruppen?

Globale Gruppen	Lokale Gruppen

15. Welche lokalen Benutzer (außer den NT-Systembenutzern) sind auf welchen Rechnern der Domäne angelegt?

Rechnername	PDC/ BDC / Workstation	Benutzernamen

16. Welche Administratoren und Benutzer haben welche RAS Zugriffsrechte?

Name / Funktion / Rechner	Kein Rückruf	Vom Anrufer festg.	Vorbelegt	Zeiteinschr.

17. Gibt es für Benutzer Einschränkungen in Bezug auf die Tageszeit der Anmeldung oder bestimmte Rechner?

Name / Funktion / Rechner	Tageszeiteinschr. Von/bis	Rechnereinschränkung

## ***Richtlinien***

18. Welche Einstellungen haben die Kontenrichtlinie des PDC?

19. Gibt es Rechner die anderen Kontenrichtlinien haben? Welche?

20. Welche Gruppen/Benutzer haben welche Benutzerrechte am PDC?

21. Gibt es Rechner, die andere Einstellungen für die Benutzerrechte haben? Welche?

22. Welche Einstellungen haben die Überwachungsrichtlinien des PDC?

23. Gibt es Rechner die andere oder keine aktiven Überwachungsrichtlinien haben? Welche?

24. Werden Systemrichtlinien verwendet ? Für welche Benutzer, Gruppen/Computer?

25. Werden Richtlinienvorlagen verwendet ? Für welche Benutzer, Gruppen/Computer?

26. Welche Arten von Benutzerprofilen werden verwendet?

Benutzer	serverbasiert persönlich	serverbasiert obligatorisch	lokal	Gruppenzugehörigkeit

## ***Überwachung***

27. Welche Ressourcen im System werden überwacht? Ja Rechnername (Typ)

Dateien

Verzeichnisse  
Drucker  
Registry  
Login-Verzeichnis  
Profilverzeichnis

28. Werden die Registry-Editoren überwacht? Ja Nein

29. Welche Systemprogramme werden überwacht? Name / Rechner

30. Welche Anwendungsprogramme werden überwacht? Name / Rechner

### **Personenbezogene Daten**

31. Werden in der Domäne personenbezogene Daten in Anwendungen verarbeitet und/oder gespeichert?

Ja Nein

32. Wenn ja, auf welchen Rechnern?

33. Wer sind die Besitzer dieser Dateien?

Rechner	Verzeichnis/Datei	Besitzer

34. Welche Gruppen/Benutzer haben welche Zugriffsrechte auf diese personenbezogenen Daten?

Gruppe/Benutzer	Verzeichnis/Datei	Zugriffsrechte

35. Auf welcher Ebene wird eine Überwachung solcher Dateien durchgeführt?

Verzeichnisebene Dateiebene keine Ebene

36. Welche Aktionen werden überwacht?

	Erfolgreich	Fehlschlag
Lesen(R)		
Schreiben(W)		
Ausführen(X)		
Löschen(D)		
Berechtigung Ändern(P)		
Besitz übernehmen(O)		

37. Sind Verzeichnisse mit personenbezogene Daten im Netzwerk freigegeben? Welche?

Ja Nein Verzeichnisname/Rechner Freigabename

38. Welche Rechte sind an wen im Rahmen der Freigabe vergeben worden?

Freigabename	Gruppe/Benutzer	Zugriffsrecht

39. Sind diese Dateien verschlüsselt?

Ja Nein teilweise

40. Welche Verzeichnisse enthalten verschlüsselte Dateien?

Rechner / Verzeichnisname



41. Sind Zugriffe mit dem Remote Access Service (RAS) auf Verzeichnisse mit personenbezogenen Daten erlaubt?

Ja                      Nein

41. Wenn ja, welche ?

Rechner	Verzeichnisname	RAS-Zugriff (frei/Rückruf/)
---------	-----------------	-----------------------------

42. Wenn ja, wird der Zugriff während der Übertragung mit RAS verschlüsselt?

Ja                      Nein

### ***Ereignisanzeige***

43. Werden Protokolle der Ereignisanzeige vor dem Löschen archiviert?

Ja              Nein              Rechner/Pfad

44. Werden die gespeicherten Log-Dateien in einem sicheren Verzeichnis (gesetzte Zugriffsrechte und Überwachung) abgelegt?

Ja                      Nein

45. Gibt es einen speziellen EDV Revisor für die Kontrolle und Wartung der EventLog-Protokolle?

Ja                      Nein

### ***Kontrolle der aktuellen und gespeicherten Ereignisanzeige des PDC/des lokalen Rechners nach Fehlercodes***

46. Sind folgende (beispielhafte) Fehlercodes in den Ereignisanzeigen zu finden?

Code	Erklärung	Aufgetreten	Datum
512	Datum und Uhrzeit des Systemstarts		
513	Datum und Uhrzeit des Systemabschlusses (Shutting Down)		
517	Ereignisanzeige gelöscht		
529	Erfolgloser Login - Unbekannter Benutzer oder Falsches Paßwort		
530	Erfolgloser Login - Zugriffsversuch außerhalb der zulässigen Zeiten		
531	Erfolgloser Login - Konto gesperrt		
532	Erfolgloser Login - Kontoberechtigung abgelaufen		
533	Erfolgloser Login - Benutzer darf sich nicht an diesem Computer anmelden		
535	Erfolgloser Login - Paßwort abgelaufen		
539	Erfolgloser Login - Konto gesperrt		
560	Zugriff auf Objekt		
608	Benutzerrecht wurde zugewiesen		
609	Benutzerrecht wurde gesperrt		
610	Richtlinienänderung Vertraute Domäne hinzugefügt		
611	Richtlinienänderung Vertraute Domäne entfernt		
612	Änderung der Überwachungsrichtlinien		
624	Benutzer - Konto wurde angelegt		
625	Benutzer - Kontentyp wurde geändert (lokal - serverbasiert)		
626	Benutzer - Konto wurde freigeschaltet		
628	Benutzer - Paßwort wurde gesetzt		
629	Benutzer - Konto wurde gesperrt		
630	Benutzer - Konto wurde gelöscht		
631	Globale Gruppe - Neue Gruppe		
632	Globale Gruppe - Mitglied hinzugefügt		
633	Globale Gruppe -		

634	Globale Gruppe - Gruppe gelöscht		
635	Lokale Gruppe - Neue Gruppe		
636	Lokale Gruppe - Mitglied hinzugefügt		
637	Lokale Gruppe - Mitglied entfernt		
638	Lokale Gruppe - Gruppe gelöscht		
639	Lokale Gruppe - Gruppe geändert		
641	globale Gruppe - Gruppe geändert		
642	Benutzer - Konto wurde geändert		
643	Domänen Politik geändert		
1002	serverbasiertes Profil - Benutzer wurde obligatorisches Profil zugewiesen		
1003	serverbasiertes Profil - Das obligatorische Profil wurde nicht gefunden		
1018	serverbasiertes Profil - Update von diesem Rechner nicht erlaubt		

47. Wenn einer der zuvor aufgelisteten Codes gefunden wurde:

Welche Maßnahmen wurden/werden eingeleitet?

---

## **RAS**

48. RAS-Berechtigung

Welche Benutzer haben welche RAS-Berechtigung?

Benutzer	Kein Rückruf	Anrufer bestimmt	vorgegebene Rückrufnummer
----------	--------------	------------------	---------------------------

Kontrolle der RAS Verbindungen

Code	Erklärung	Ja trifft zu	Datum
20016	Benutzer konnte sich in der RAS Verbindung nicht authentisieren		
20017	Benutzer hat sich erfolgreich über RAS angemeldet		
20093	Rückrufversuch des RAS Servers ist fehlgeschlagen		

49. Wenn einer der zuvor aufgelisteten Codes gefunden wurde:

Welche Maßnahmen wurden/werden eingeleitet?

## ■ Literaturverzeichnis

---

### 1.1 Literatur (deutsch)

- Brotz, Karin und Föckler, Philipp; Security unter Windows NT 4, Heidelberg 1997
- Dapper, Thomas u.a.; Windows NT 4.0 im professionellen Einsatz, Band 1 + 2, 2. Auflage, Hanser Verlag 1997
- Kuppinger, M.; Microsoft Windows NT im Netzwerk, Version 4: Planung Installation und Management von Netzwerken mit Windows NT Server und Workstation, Version 4; Microsoft Press Deutschland, Unterschleißheim, 2. Auflage 1998
- Mansfeld, Godehard; Windows NT 4 Referenzen; 1997
- Microsoft, Windows NT 4.0 Training Netzwerk-Administration, Microsoft Press 1997
- Pearce, Eric; Windows NT in a nutshell, deutsche Übersetzung von Andreas Roeschies, O'Reilly 1998
- Zenk, Andreas; Sicherheit unter Windows NT 4.0, Addison-Wesley 1997

### 1.2 Literatur (englisch)

- Espinola, Micheal ; The Hardening of Microsoft Windows NT V4, Rev 1, Bezug nur direkt beim Autor über das Internet, email : micheale@ix.netcom.com
- Kaplan, Ari und Nielsen, Morten Strunge; NT 5 – The next Generation; Coriolis 1998
- Lambert, Nevon und Patel, Manisch; Windows NT Security – System Administrators Guide, PCWeek – ZD Press 1997
- Minasi, Mark; Mastering Windows NT Server 4, 5. Auflage, Sybex – Network Press 1998
- Sheldon, Tom; Windows NT Security Handbook, McGraw-Hill 1997
- Windows NT Magazine : [www.winntmag.com](http://www.winntmag.com). Sehr gutes Magazin, alle (!) Hefte werden komplett mit dreimonatiger "Verzögerung" im Internet veröffentlicht werden (inklusive Suchmaschine)

### 1.3 Internet Ressourcen (deutsch)

- Windows NT – Einführung und Konzepte von Georg Lucas und Bernhard Tritsch [www.igd.fhg.de/www/grz/mswin/index.html#Seminar](http://www.igd.fhg.de/www/grz/mswin/index.html#Seminar)
- International Network of Institutions for Computer Graphics, Windows NT Development and Solution Center : [www.igd.fhg.de/www/grz/devnsol/index.html](http://www.igd.fhg.de/www/grz/devnsol/index.html)

### 1.4 Internet Ressourcen (englisch)

- Windows NT FAQ , [www.savilltech.com/download/faqcomp.zip](http://www.savilltech.com/download/faqcomp.zip) oder [www.ntfaq.com](http://www.ntfaq.com)
- Information securit Resources (Idaho State University) : <http://gandalf.isu.edu/security/security.html>
- Verschiedene excellente Tools : [www.sysinternals.com/util.htm](http://www.sysinternals.com/util.htm)
- Trusted Systems : [www.trustedsystems.com](http://www.trustedsystems.com)
- Sicherheitstools : [www.somar.com](http://www.somar.com)

### 1.5 Electronic Newsletters (deutsch)

- Windows NT Newsletter (PC Magazin) : [www.wekanet.de/news](http://www.wekanet.de/news)

### 1.6 Electronic Newsletters (englisch)

- Sunbelt Windows NTools E-News : [www.sunbelt-software.com](http://www.sunbelt-software.com)

- ESI Tech Support Mail List : [www.execsoft.com/tech-support](http://www.execsoft.com/tech-support)
- Windows NT Magazin UPDATE , wöchentlicher newsletter.  
[www.winntmag.com/update](http://www.winntmag.com/update)

### 1.7 Windows NT Shareware (deutsch)

- ELWIZ (EventLogWizard) und NT – Eventlog : [rcswww.urz.tu-dresden.de/~fh/nt/eventlog/deutsch.htm](http://rcswww.urz.tu-dresden.de/~fh/nt/eventlog/deutsch.htm)
- Security Manager [home.t-online.de/home/wispro/secumgr.html](http://home.t-online.de/home/wispro/secumgr.html)
- Visual Netinfo : Falk Schmal und Torsten Spreiz: [www-rnks.informatik.tu-cottbus.de/~fsch/deutsch/netinfo.htm](http://www-rnks.informatik.tu-cottbus.de/~fsch/deutsch/netinfo.htm)

### 1.8 Windows NT Tools (englisch)

- Somarsoft: [www.somarsoft.com](http://www.somarsoft.com)
- Aelita Software : [www.ntsecurity.com/products/config\\_save](http://www.ntsecurity.com/products/config_save)

## ■ Schlagwortverzeichnis

### **S**

§ 9 BDSG

### **A**

Abschottung  
AD (Active Directory)  
Administration, Checkliste  
Administratorpaßwort sperren  
ANMELDEN AN  
Anwendungsprotokoll  
Apple Macintosh  
Arbeitsgruppenkonzept  
Aushilfskräften, Konto zeitliche begrenzen

### **B**

Begehung eines Windows NT Systems  
Begehung, Checkliste für eine  
Begehung, Dokumentation der  
Benutzer, lokale  
Benutzermanager für Domänen  
Benutzerprofile  
Benutzerverwaltung, Checkliste  
BETA-Version

### **C**

C2 33  
Checkliste, Hinweise zur Bearbeitung  
Complete-Trust-Modell

### **D**

Dateiebene, Zugriffsbeschränkung  
Datenschutz, § 9 BDSG  
Domänen-Administratoren  
Domänenbenutzer  
Domänen-Benutzer  
Domänenkonzept planen  
Domänenmodelle  
Domänenorganisation  
Druck-Operatoren  
DumpACL, Sharewareprogramm

### **E**

Ereignisanzeige  
Ereignisanzeige, Checkliste

Ereignisanzeige, Meldungen der  
Ereignisanzeige, Symbole der  
Ereignisprotokolle, Archivierung der  
Ereignisprotokolle, Speicherort  
Ereignisprotokoll, RAS-Ereignisse  
ERSTELLER-BESITZER  
EventLog Wizard

### **F**

Freigabeberechtigungen  
Freigaben  
Freigaben, versteckte

### **G**

Gast  
Gruppe REVISION  
GRUPPEN  
Gruppen, globale  
Gruppen, lokale  
Gruppen, vordefinierte  
GRUPPEN, Zuordnung im Benutzermanager

### **H**

Hauptbenutzer  
HKEY\_CLASSES\_ROOT  
HKEY\_CURRENT\_CONFIG  
HKEY\_CURRENT\_USER  
HKEY\_LOCAL\_MACHINE

### **I**

Informationsgespräche mit dem Arbeitgeber  
INTERAKTIV  
J  
JEDER

### **K**

Kennwortchronik  
Kommandozeilen-Programme  
Konten-Operatoren  
KONTO, Zuordnung im Benutzermanager

### **L**

Login-Skripte  
Löschung der Konten der Administratoren

### **M**

Master-Domänen-Modell  
MMC (Management Console)  
Multiple-Master-Domäne

### **N**

NET Befehle  
Netinfo, Sharewareprogramm  
NETLOGON  
Netware  
NETZWERK  
Novell-Laufwerke  
NT Installations-CDs  
NT Organisations- und Sicherheitskonzept  
NT, echnische Einrichtung gemäß § 87.1.6 BetrVG  
NTFS  
NTFS-Berechtigungen  
ntuser.dat  
NTUSER.dat

### **O**

Online-Hilfen  
OS/2

### **P**

Paßwortgestaltung  
Peer-to-Peer-Netzverbindung  
Peer-to-Peer-Netzwerk, C2  
Personenbezogene Daten, Checkliste  
primären Domänen-Controller  
Profil, mandatory  
PROFIL, Zuordnung im Benutzermanager  
Profile, serverbasierende  
Profiles-Verzeichnis  
Programm, nützliche  
Protokolldateien, Speicherort

### **R**

RAS  
RAS, Zuordnung im Benutzermanager  
RAS, Checkliste  
RAS-Server  
RAS-Verbindungen  
Rechtevergabe, RAS  
regedt  
Regedt

## REGEDT

Registry-Überwachung  
aktivieren mit  
Registrierdatenbank  
Registry  
Replikations-Operatoren  
Revisions/Auditor-Konto  
Richtlinien für Konten  
Richtlinien, Checkliste  
Rückwahlnummer

## S

SAM  
SCE (Security Configuration  
Editor)  
Security Access Manager  
Server-Operatoren  
Sharewareprogramme für  
NT  
Sicherheitsmanager  
Sharewareprogramm  
Sicherheitsmerkmale von  
Windows NT  
Sicherungs-Domänen-  
Controller  
Sicherungs-Operatoren

Single Domänen Modell  
Sub-Administratoren  
Subadministratorenkonten  
Systemprotokoll  
Systemrichtlinien

## T

TCO  
Thin Clients  
Trivialpaßwörter

## Ü

Überwachung aktivieren  
Überwachung und Kontrolle  
Überwachung, Checklisten  
Überwachungs- und Kon-  
trollmöglichkeiten bei  
Thin Clients  
Überwachungsrichtlinien

## V

Vertrauensbeziehungen  
VOLLZUGRIFF  
VOLLZUGRIFF, Entzug des

## W

Windows 2000  
Windows 95  
Windows NT 5  
Windows NT Messages  
Windows NT Server  
Windows NT Server  
Enterprise Edition  
Windows NT Small Business  
Server  
Windows NT Terminal  
Server  
Windows NT Vereinbarung,  
Beispiel  
Windows NT Workstation

## Z

ZAK (Zero Administration  
Kit)  
ZEITEN, Zuordnung im  
Benutzermanager  
Zugriffsbegrenzung, zeitlich

---

Dieses Dokument wurde von der forba Partnerschaft herausgegeben. Es stellt einen Auszug aus einer forba-Veröffentlichung dar und soll einen Überblick über die Veröffentlichung vermitteln.

Für weitere Informationen wenden Sie sich bitte direkt an forba:

**forba Partnerschaft**

Dominicusstraße 3  
10823 Berlin

Tel.: 030 - 78 00 86 - 0  
Fax: 030 - 78 00 86 - 19

Web: [www.forba.de](http://www.forba.de)  
E-Mail: [forba@forba.de](mailto:forba@forba.de)

Diesen Artikel können Sie auch direkt herunterladen unter  
[www.forba.de/veroeffentlichungen/handbuch-nt.pdf](http://www.forba.de/veroeffentlichungen/handbuch-nt.pdf)