Kürschner, Michael; Teppich, Helmut

Book

Windows NT: Handbuch für Betriebsräte. Regelungsbedarf und Kontrollmöglichkeiten

edition der Hans-Böckler-Stiftung, No. 19

Provided in Cooperation with:
The Hans Böckler Foundation

Suggested Citation: Kürschner, Michael; Teppich, Helmut (1999) : Windows NT: Handbuch für Betriebsräte. Regelungsbedarf und Kontrollmöglichkeiten, edition der Hans-Böckler-Stiftung, No. 19, ISBN 3-92820-492-0, Hans-Böckler-Stiftung, Düsseldorf

This Version is available at:
https://hdl.handle.net/10419/116271

19

Michael Kürschner
Helmut Teppich

Windows NT: Handbuch für Betriebsräte

edition der
Hans **Böckler**
Stiftung

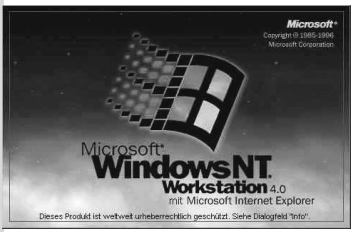
Michael Kürschner
Helmut Teppich

Windows NT:

Handbuch

für Betriebsräte

Regelungsbedarf und Kontrollmöglichkeiten



edition der Hans-Böckler-Stiftung 19

Michael Kürschner arbeitet als Informatiker in einem Rechenzentrum.

Helmut Teppich ist Partner der FORBA Partnerschaft und arbeitet dort als Technologieberater (h.teppich@forba.de / www.forba.de)

Bertha-von-Suttner-Platz 1, 40227 Düsseldorf
Buchgestaltung: Horst F. Neumann Kommunikationsdesign, Wuppertal
Produktion: Der Setzkasten GmbH, Düsseldorf
Printed in Germany 1999
ISBN 3-928204-92-0
Bestellnummer: 13019

INHALT

1.1 VORWORT

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 , insbesondere was ihre Beteiligungsrechte anbelangt. 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. Fragestellungen zu den mitbestimmungspflichtigen auf Windows NT aufsetzenden sogenannten Back Office-Programmen (Exchange, SQL Server, SMS, IIS) werden aus Platzgründen ebenfalls nicht behandelt. Zur Vertiefung dieser Details wird auf die Quellen im Anhang verwiesen.

Zur Erstellung dieses Buches wurden Pentium-Rechner mit NT Workstation 4 Servicepack P3 (Build 1381) und NT Server 4 Servicepack 3 (Build 1381) eingesetzt.

Die mit diesem Zeichen versehenen Absätze sind Hinweise auf Themen, die unseres Erachtens von der Interessenvertretung beachtet werden sollen.

Die mit diesem Zeichen versehenen Absätze sind Vorschläge, wie mit einer Situation oder einem Thema von der Interessenvertretung umgegangen werden kann.

1.2 ÜBERBLICK

Windows NT ist trotz seiner graphischen Oberfläche ein komplexes Betriebssystem. Viele Menschen verbinden graphische Oberflächen mit Einfachheit der Bedienung und Verständlichkeit eines Systems. Die Praxis sieht – nicht nur bei Windows NT – etwas anders aus. Windows NT enthält nicht nur eine graphische Oberfläche, sondern wird auch mit umfangreichen Kommandozeilenprogrammen, die auf einer DOS-ähnlichen Oberfläche (in NT heißt dies »Eingabeaufforderung«) laufen, ausgeliefert, was schon weniger Menschen bekannt ist.

Aus Sicht der Interessenvertretung ist vor allem die Kenntnis des Sicherheits- und Organisationskonzeptes von Windows NT wichtig, denn auf dieser Ebene wird die Beteiligung bei Windows NT schwerpunktmäßig ausgehandelt und ausgeübt.

Im 1. Kapitel wird ein genereller Überblick über Windows NT gegeben.

Das 2. Kapitel erläutert die grundlegenden Begriffe von Windows NT und deren Zusammenhänge, soweit sie aus unserer Sicht für die Interessenvertretung direkt relevant sind.

Im 3. Kapitel werden die Sicherheitsmerkmale von Windows NT, die Gegenstand einer Betriebsvereinbarung sein können, behandelt. Vor allem die Umsetzung von Schutzregeln für Dateien und Verzeichnisse, die Nutzung und Wirkung von Benutzerprofilen und Systemrichtlinien sowie die Installation der Überwachung und deren Kontrolle sind hier Gegenstand der Betrachtung.

Im 4. Kapitel wird Windows NT gegen die Vorgaben der Anlage zu § 9 des Datenschutzgesetzes geprüft. Es wird dargestellt, daß die zwischen Interessenvertretung und Arbeitgeber umstrittene Anwendung der technisch-organisatorischen Vorgaben des BDSG mit Windows NT zum Teil umsetzbar sind.

Im 5. Kapitel werden Argumente zusammengefaßt, warum Windows NT eine mitbestimmungspflichtige technische Einrichtung im Sinne BetrVG und der PersVG ist.

Das 6. Kapitel stellt beispielhaft einige nützliche Programme zur Begehung, Kontrolle und Administration von Windows NT vor. Die vorgestellten Programme zeichnen sich aus unserer Sicht durch sinnvolle Funktionen aus, die bei Windows NT 4 nicht implementiert wurden. Darüber hinaus stehen sie als fast voll funktionsfähige Programme im Internet zum Ausprobieren zur Verfügung.

Im 7. Kapitel werden die in den vorhergehenden Kapiteln zusammengetragenen Erkenntnisse zu einer Checkliste zusammengestellt. Bei Begehungen von NT-Systemen soll so der rote Faden nicht aus den Augen verloren werden. Die Checkliste wird durch eine Erläuterung ergänzt. Diese macht Vorschläge, wo und wie die abgefragten Informationen aus einem NT-System »herauszuholen« sind.

Kapitel 8 enthält ein Beispiel – kein Muster –, das demonstriert, welche Punkte und Themen in einer Vereinbarung zu Windows NT geregelt werden könnten.

Den Schluß bildet eine Zusammenstellung verschiedener Quellen zum Thema Windows NT. Die deutschen und englischsprachigen Quellen reichen von Büchern, über Zeitschriften, Mailing-Listen aus dem Internet bis zu Hilfsprogrammen, die kostenlos aus dem Internet beziehbar sind.

2.1 ENTWICKLUNG VON WINDOWS NT

Microsoft entwickelte in den 80er Jahren für ihr erfolgreiches Betriebssystem MS-DOS die graphische Benutzeroberfläche Windows. Unausgesprochenes Vorbild war dabei die ergonomisch vorbildliche und benutzerfreundliche graphische Oberfläche des Apple Macintosh. Anfang der 90er Jahre kam Windows 3.1 auf den Markt und wurde ein durchschlagender Erfolg. Für die Vernetzung von Windows-Rechnern wurde später eine Peer-to-Peer-Verbindung über Windows for Workgroups 3.11 ermöglicht.

Um den aufstrebenden Markt der Netzwerke zu erobern, den Novell Anfang der 90er Jahre mit seinem Produkt »Netware« dominierte, wurde Anfang der 90er Jahre das Projekt Windows NT (New Technology Operating System) gestartet. Die erste auf einem neuen 32-Bit-Betriebssystem basierende Version 3.1 von Windows NT kam Mitte 1993 als Client- (NT Workstation) und als Server-Version (NT Server) auf den Markt. Die Versionen 3.5 (1994) und 3.51 (1995) folgten, ohne aber den erhofften Erfolg zu bringen.

Mit der u. a. an die graphische Oberfläche des erfolgreichen Windows95 angelehnte Version 4 (und kostenlosen Zugaben wie dem Internet-Server IIS) gelang schließlich der kommerzielle Erfolg und Aufstieg von Windows NT. Allerdings sind die Windows NT-Administratoren nicht zwingend auf die graphische Oberfläche angewiesen, die neben der optisch einfacheren Handhabung oft auch Nachteile mit sich bringt. Kommandozeilenorientierte Befehle sind oft flexibler und ermöglichen auch eine einfachere Massendatenverarbeitung, z. B. beim Verwalten von Benutzerkonten. Deshalb arbeiten viele Administratoren gerne mit der sog. Eingabeaufforderung CMD.EXE, die zwar ein DOS-ähnliches Fenster öffnet, aber im Gegensatz zu Windows95 kein DOS beinhaltet. Windows NT installiert standardmäßig neben den graphisch orientierten Programmen zahlreiche Kommandozeilenprogramme im Stammverzeichnis WINNT \System32. Beim Blick in das Verzeichnis sind die Programme mit graphischen Oberflächen durch ihre bunten Icons leicht von den Kommandozeilenprogrammen zu unterscheiden. Die von Microsoft mit zahlreichen weiteren Verwaltungsprogrammen ausgestattete CD »Windows NT technische Referenz« und viele Dritthersteller von Ergänzungssoftware erweitern die umfangreiche Palette dieser Programme. Da diese Programme selten in der allgemeinen Computerpresse besprochen

werden, ist deren Existenz und Mächtigkeit bei vielen Benutzern und auch bei der Interessenvertretung nicht bekannt.

Kommandozeilenprogramme haben oft mächtige Funktionen für die Verwaltung, Beaufsichtigung und Betreuung von Verzeichnissen, Dateien, Benutzern und NT-Domänen (z. B. Hunderte Benutzer lassen sich aus einer Excel-Datei heraus anlegen oder ändern).

Die Interessenvertretung sollte deshalb im Rahmen der Informationsgespräche mit dem Arbeitgeber eine genaue Aufstellung der Kommandozeilenprogramme und ihrer Funktionalität einfordern und diese gegebenenfalls auch in der Vereinbarung dokumentieren.

Neben den beiden ursprünglichen NT-Versionen existieren inzwischen weitere Server-Versionen: Windows NT Server Enterprise Edition, Windows NT Small Business Server (SBS) und der Windows NT Terminal Server. Die SBS ermöglicht (im Unterschied zur Standard Server-Version) nur maximal 25 Benutzern die gleichzeitige Verbindung mit dem Server und kann auch keine Vertrauensbeziehungen zu anderen Domänen aufbauen. Dafür werden im Lieferumfang kostenlos weitere Server-Programme aus dem BackOffice-Bereich mitgeliefert: Exchange Server, SQL Server, Fax Server und Modem Sharing Server.

Mit der Windows NT Terminal Server Edition bietet Microsoft seine Lösung in der Diskussion um die TCO (Total Cost of Ownership = Kosten des Unterhalts von DV-Systemen) und die sogenannten Thin Clients (dünne Clients) an. Im Unterschied zu den NT Server-Versionen wird hier kein Client/Server-System im klassischen Sinne aufgebaut. Statt dessen greifen die Clients auf die servergespeicherten Programme und Daten zu. Auf dem Terminal Client ist nur noch ein Minimum an Programmcode vorhanden, z. B. für die Oberfläche und die Kommunikation. Eigene Plattenkapazität wurde beim Clientrechner weggelassen (deshalb auch dünne Clients). Bemerkenswert ist, daß so mit Windows for Workgroups-Rechnern Office 97 lauffähig ist.

Die Einrichtung von NT-Terminals wird bezüglich der Überwachungs- und Kontrollmöglichkeiten oft falsch eingeschätzt. Da die gesamte Datenverarbeitung bei dieser NT-Variante auf dem Server verläuft, werden im Gegensatz zur Workstation, die sich oft nur am Server anmeldet, alle Benutzeraktivitäten auf dem Server kontrollierbar.

Da die Zugriffsrechte hier sehr genau geplant und vergeben werden (sollten), sollte die Interessenvertretung die für die Terminal-Server-Installation notwendigerweise erarbeiteten Planungsunterlagen zur Information anfordern

2.2 SYSTEMTYPEN

Seit der ersten Version von Windows NT existieren nur zwei grundsätzliche Systemtypen: die Windows NT Workstation und der Windows NT Server. Bei der Diskussion um NT-Netze und den Client/Server-Ansatz von Windows NT wird oft übersehen, daß Windows NT – bei beiden Systemtypen – oft auch als alleinstehendes System zum Einsatz kommt. Vor allem bei Spezialanwendungen, die keine weitere Verbindung zu anderen Systemen benötigen, wird Windows NT in dieser Form eingesetzt.

Die NT Workstation wird vor allem als Client in Netzwerken eingesetzt. Sie ist dadurch gekennzeichnet, daß sie nicht zu Zwecken der zentralen Benutzerverwaltung in einem Netzwerk benutzt werden kann. Die Workstation ist nur in der Lage, die auf ihr eingerichteten lokalen Gruppen und Benutzer zu verwalten. Dennoch können andere Rechner auf die Workstation in einer Peer-to-Peer-Netzverbindung zugreifen. Eine Peer-to-Peer-Verbindung ermöglicht den beteiligten Rechnern, Daten miteinander auszutauschen und Verzeichnisse für die gegenseitige Benutzung freizugeben. Die Anzahl anderer Rechner (Windows 95/98 oder andere NT Workstations), welche in einem Peer-to-Peer-Netz gleichzeitig auf eine NT Workstation zugreifen können, ist lizenzmäßig auf zehn gleichzeitige Rechnerzugriffe begrenzt. Eine Workstation kann per Modem/ISDN nur eine RAS-Verbindung (Remote Access Service) zu einem entfernten Rechner aufbauen. Es stehen keine Server-Funktionalitäten zur Verfügung, d. h., daß z. B. Vertrauensstellungen zu anderen Rechnern/Domänen von der Workstation aus nicht definiert werden können. Bei der Betrachtung dieser scheinbaren Einschränkungen muß aber berücksichtigt werden, daß in vielen Betrieben bzw. vielen Arbeitsbereichen überhaupt keine Notwendigkeit besteht, mehr als das Leistungsspektrum der Workstation abzufordern, zumal die NT-Sicherheitsfunktionen zur Verfügung stehen.

Der NT-Server hat (in der Standardversion) keine vorgegebenen technischen Begrenzungen des gleichzeitigen Client-Zugriffs. Soweit der Server bei der Installation als primärer Domänen-Controller festgelegt wurde, verwaltet er alle Gruppen und Benutzer in einer Domäne. Der Server als primärer Domänen-Controller (PDC) kann Vertrauensbeziehungen zu anderen Domänen herstellen. Bis zu 255 gleichzeitige RAS-Verbindungen (Fernzugriffe von außerhalb der Domäne über Modem oder ISDN) lassen

sich am Server betreiben. Als Clients können DOS-, Windows for Workgroups-, Windows 95-, Windows 98-, Apple Macintosh- oder OS/2-Rechner angemeldet werden. Der Server auch kann als Gateway zu Netware-Netzen sowie als Datei-Server in Netware-Netzen fungieren.

Die Sicherheits- und Überwachungsfunktionen stehen bei Server und Workstation in fast gleichem Umfang zur Verfügung. Zum Aufbau und zur Überwachung einer, zwar nicht optimalen, aber im Vergleich zu Windows 95 oder Windows 98-Rechnern sicheren Umgebung, z. B. zur Verarbeitung personenbezogener Daten, sind Workstation wie Server aus unserer Sicht deshalb prinzipiell gleich gut verwendbar. Die Kritik an NT wegen seiner Sicherheitsmängel ist berechtigt, darf aber nicht darüber hinwegtäuschen, daß viele spektakuläre Meldungen erst möglich wurden, weil die NT-eigenen Schutzmechanismen, aber auch die technisch-organisatorische Sicherung von Servern und Workstations, unzureichend realisiert waren. Ein großer Teil der Angriffsmöglichkeiten wird in einem betrieblichen Netzwerk ohne Internet-Zugang gar nicht auftreten können.

2.3 ORGANISATIONSKONZEPTE

Soll ein Client/Server-Netzwerk auf Windows NT-Basis aufgebaut werden, sind vorher detaillierte Planungen zwingend notwendig. Um grundlegende Festlegungen über die Art des Domänenkonzeptes treffen zu können, muß bereits in der Konzeptionsphase überlegt werden, wie viele Standorte vernetzt werden sollen, wie viele Rechner in das Netz eingebunden werden sollen, wie viele Benutzer im Netzwerk verwaltet werden sollen und wie zentral oder dezentral sie verwaltet werden sollen.

Kurze Zeitverläufe bei der Installation deuten auf ungenügende Planung bei den Fragen der Zugriffssicherung hin. Die Installation von NT-Systemen wird – wegen der Komplexität von NT – immer einen längeren Vorlauf haben, da nicht nur NT, sondern auch die Programme installiert und gegebenenfalls ein Netzwerk aufgebaut oder ausgebaut wird.

Für eine Beteiligung der Interessenvertretung im Planungsstadium und einer Berücksichtigung von deren Vorschlägen ist nach unserer Erfahrung somit immer genügend Zeit. Die Interessenvertretung sollte sich vom Arbeitgeber bei der Bearbeitung eines Zustimmungsantrages nicht unter Zeitdruck setzen lassen.

Eine weitere Voraussetzung für die erfolgreiche Installation eines NT-Netzes und dessen Betrieb ist ein »Windows NT-Organisations- und Sicherheitskonzept«. In einem solchen Konzept müssen – vorab und unter Beteiligung der Interessenvertretung und des Datenschutzbeauftragten – grundsätzliche Entscheidungen getroffen und deren Umsetzung organisiert werden. Zum Beispiel: Wo werden welche Programme, wo welche Daten gespeichert? Wer darf/darf nicht in welchem Umfang und auf welchem Weg Zugriff auf diese Programme und Daten nehmen? Wer darf/darf nicht welche Ressourcen nutzen? Wie soll eine Sicherheitsstrategie aussehen? Sollen die Überwachungsmöglichkeiten von Windows NT genutzt werden? Inwieweit sollen die Benutzer die Möglichkeit bekommen, sich »ihren« Rechner in der Oberfläche selbst einzurichten? Microsoft stellt dafür ausführliche Planungs- und Installationshilfen zur Verfügung.

Auf den Installations-CDs für Server und Workstation und zu fast allen NT Programmen werden z. B. Online-Hilfe-Dateien wie die Datei Server.hlp mitgeliefert. Diese Hilfe-Dateien passen oft auf eine Diskette und lassen sich auf jedem Windows-Rechner lesen.

Als erste Informationsquelle für die Interessenvertretung bzw. den Einstieg ins Thema Windows NT sind die Online-Hilfen aus unserer Erfahrung zu empfehlen und sollten vom Arbeitgeber abgefordert werden.

Copyrightgründe, die gegen eine Vervielfältigung innerhalb des Betriebes sprechen, sind manchmal ein Argument gegen die Weitergabe der Hilfe-Dateien an die Interessenvertretung. Diese Gründe sind unseres Erachtens aber nur vorgeschoben und außerdem bezüglich des Copyrights unzutreffend, da der Betriebsrat Teil des Betriebes ist, der die Lizenz erworben hat.

Alle auf einem NT-Rechner gespeicherten Hilfe-Dateien (aber nicht nur die) lassen sich mit einem Befehl auf allen Platten eines NT-Rechners leicht finden: START – SUCHEN – DATEI/ORDNER – <*.hlp> STARTEN und alle Hilfedateien werden aufgelistet. Ein Klick auf das Icon der gewünschten Hilfedatei öffnet diese.

Abbildung 1: Planungshandbuch

Abbildung 2: Netzwerkhandbuch

2.3.1 Das Arbeitsgruppenkonzept

Ein zentrales Problem aller Netze besteht in der Organisation und Verwaltung der vernetzten Rechner und ihrer Benutzer. Microsoft hat dafür zwei Konzepte entwickelt, die für das Grundverständnis von Windows NT (zumindest bis zur Version 4) wichtig sind.

Die Arbeitsgruppe ist die einfachste Strukturierungsform in einem Windows NT-Netzwerk. Sie wurde bereits – als sogenanntes Peer-to-Peer-Netzwerk – unter Windows 3.11 (Windows for Workgroups) realisiert und findet heute noch (vor allem bei Einsatz von NT Workstations) Anwendung.

Windows NT muß nicht als Client/Server-System installiert werden! In vielen Betrieben oder Abteilungen ist dies »eine Nummer zu groß«. Außerdem müßte in einem »echten« Netz kompetente Betreuung durch Administratoren bereitgestellt werden.

Die Interessenvertretung sollte umgehend eine Begehung des Systems machen (siehe auch Kapitel 8).

Im Arbeitsgruppenkonzept ist keine zentrale Verwaltung der Benutzer mehrerer Rechner möglich. So muß auf jedem einzelnen Rechner (dies können auch Server sein!) der Arbeitsgruppe eine eigene Benutzerdatenbank der berechtigten Benutzer und ihrer Rechte auf diesem Rechner existieren und gepflegt werden. Es müssen für jeden später dazukommenden Rechner bzw. jeden neuen Benutzer Freigaben auf Verzeichnisse, Dateien und Ressourcen eingerichtet werden. Da bei jeder Änderung von Benutzern oder Rechnern aufwendige Pflegearbeiten notwendig sind, ist dieses Konzept nur in sehr kleinen Netzen (bis ca. 25 Benutzer) praktikabel. Es gibt aber in jedem Betrieb Bereiche oder Abteilungen, die sich auch bewußt vom »großen« Gesamtnetz fernhalten und ihre eigenen Strukturen verwalten und pflegen. Dies schafft Abstand zu den Begehrlichkeiten anderer Personen und gewährleistet darüber hinaus Schutz vor ungebetenem Zugriff.

2.3.2 Das Domänenkonzept

Eine Domäne ist eine logische Netzwerkstruktur, d. h. sie spiegelt eine vom Arbeitgeber gewollte Organisation der betrieblichen Rechner (als Vertreter der jeweiligen Arbeitsplätze) auf einer technischen Basis dar. Eine Domäne ist dadurch gekennzeichnet, daß

alle Benutzer (alle Rechner) in einer Stelle der Domäne zentral angelegt und verwaltet werden. Die Domäne kann sich auch über mehrere physikalische Netzwerke erstrecken. Es kann aber auch in einem physikalischen Netzwerk mehrere Domänen geben. Die Installation einer Domäne vereinfacht die Strukturierung und Verwaltung vieler Benutzer, vieler Rechner und vieler Ressourcen entscheidend.

Die Benutzerverwaltung einer Domäne erfolgt auf dem sogenannten primären Domänen-Controller (PDC). Es existiert in einer Domäne nur ein einziger PDC, damit es keine widersprüchlichen oder doppelten Benutzerkonten gibt. Die Benutzer der Domäne sind mit ihren Benutzerkonten und Gruppenzugehörigkeiten ausschließlich in der Benutzerdatenbank (SAM = Security Access Manager) des PDC angelegt.

Jeder Benutzer kann bei der Anmeldung an seinem Rechner immer auswählen, ob er sich an der Domäne oder nur lokal am eigenen Rechner anmelden möchte. Da es keine Zwangsanmeldung an eine Domäne gibt, hat trotz der zentralen Benutzerverwaltung durch den PDC jeder NT-Rechner in der Domäne auch seine eigene lokale Benutzerdatenbank. Damit kann sich der Benutzer im Fall des Ausfalls des PDC immer noch an »seinem« Rechner anmelden und arbeiten.

Meldet sich ein Benutzer an der Domäne an, so wird seine Identität mit Namen und Paßwort an der Benutzerdatenbank des PDC geprüft. Die Übertragung des Paßwortes zum PDC erfolgt dabei verschlüsselt. Im Fall entfernter Rechner in anderen physikalischen Netzen oder an anderen Standorten kann es durch die Entfernung zu langen Anmeldezeiten kommen. Auch kann eine Anmeldung scheitern, weil die Leitung unterbrochen ist. Um solche Probleme zu unterbinden, werden in großen oder entfernten Domänenstandorten sogenannte Sicherungs-Domänen-Controller (BDC = Backup Domain Controller) eingesetzt. Diese Rechner replizieren (= kopieren) die Benutzerdatenbank des PDC in einem vorgegebenen Rhythmus auf alle BDCs. Damit werden alle auf dem PDC angelegten Benutzer und ihre Gruppenzugehörigkeit sowie ihre Rechte in der Domäne auf den BDC »kopiert« und aktualisiert. Die Anmeldezeiten verkürzen sich bei einer Anmeldung am »nahen« BDC stark.

Neben PDC- und BDC-Servern können auch NT-Server, die keine Verwaltungsrolle in der Domäne haben, ins Netz eingebunden werden. In der Regel handelt es sich dabei um Server, die nur spezielle Aufgaben erfüllen, z. B. Mailserver oder Datenbankserver.

Grundsätzlich lassen sich vier Domänenmodelle unterscheiden:

Das Single-Domänen-Modell

Das aufwandsmäßig einfachste Domänenkonzept ist das der »einfachen Domäne« oder Single-Domänen-Modell. Am PDC werden alle Benutzer der Domäne angelegt und verwaltet. Die Benutzer werden in der Domäne in sogenannten globalen Gruppen

zusammengefaßt. Alle Rechner (Clients und einfache Server) des Netzes werden Mitglieder der Domäne und stellen ihre Ressourcen der Domäne zur Verfügung. Ressourcen sind Laufwerke, Verzeichnisse, Dateien und Drucker. Den lokalen Gruppen auf den Clients werden die Rechte an Ressourcen auf den jeweiligen Clients zugewiesen. Die am PDC angelegten globalen Gruppen werden zu Mitgliedern der lokalen Gruppen der Clients gemacht und erhalten so die Objektrechte ihrer Gruppe. Die Benutzerpflege auf den einzelnen Clients wird dadurch drastisch reduziert. Dieses Modell wird sinnvoll bei einer geringen bis mittleren Benutzeranzahl (max. 500 Benutzer) eingesetzt.

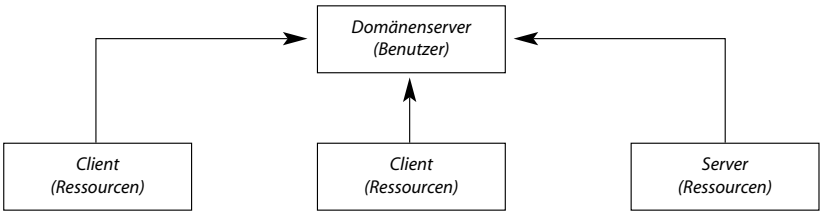


Abbildung 3: Single-Domänen-Modell

Das Modell der einfachen Domäne ist dann kritisch zu sehen, wenn in einer Domäne Betriebsbereiche (also auch der Personalbereich) zusammen organisiert werden.

Alle Benutzer dieses Domänen-Modells haben nach der Installation Zugriff auf alle Ressourcen ihrer Domäne, wenn ihnen diese Rechte nicht explizit entzogen werden. Die standardmäßige Installation von Microsoft ist bezüglich der Rechtevergabe unter Sicherheitsaspekten mangelhaft. In der Praxis hat sich immer wieder gezeigt, daß die standardmäßig vorhandenen Werkzeuge von Windows NT zur Abschottung von sensiblen Daten mit der Begründung der mangelnden Personalkapazität zur Bewältigung des notwendigen Organisations- und Pflegeaufwandes nicht angewendet werden.

Die Interessenvertretung sollte sich die Organisation und Arbeitsteilung in der Administration genau ansehen. Ein nachvollziehbares formales Freigabeverfahren für die Erteilung von Benutzerkonten und Rechten sollte eingerichtet werden.

Das Single-Domänen-Modell bietet sich andererseits dann an, wenn der Personalbereich innerhalb eines Unternehmens von allen anderen DV-Systemen abgesichert arbeiten soll.

Das Master-Domänen-Modell

Die Weiterführung des vorstehenden Ansatzes stellt das Master-Domänen-Modell dar. Das Master-Domänen-Modell wird dann eingesetzt, wenn mehrere Domänen in einem Netzwerk vorhanden sind, z. B. mehrere weit entfernte Niederlassungen, und die Verwaltung der Benutzerkonten dennoch zentral erfolgen soll. Dabei vertrauen alle beteiligten sogenannten sekundären oder Ressourcen-Domänen einseitig der Master-Domäne. Es handelt sich hier um eine einseitige Vertrauensstellung. Diese Konstruktion wird oft dann eingesetzt, wenn in einem Unternehmen eine zentrale DV-Abteilung existiert, vor Ort aber keine ausreichende DV-Kompetenz vorhanden ist. Bei Anwendung des Master-Domänen-Modells werden keine lokalen Administratoren benannt, sondern die Domänen-Administratoren der zentralen Domäne werden Mitglieder der lokalen Gruppe der Administratoren der vertrauten Domäne.

Die Verwaltung der Rechte an Objekten/Ressourcen (Freigabe oder Entzug von Platten, Verzeichnissen, Druckern) in den sekundären oder Ressourcen-Domänen kann (muß aber nicht) durch eigene Administratoren oder Sub-Administratoren (siehe Abschnitt 2.4.3) erfolgen. Denn auch diese Tätigkeit kann grundsätzlich durch die zentrale Administration abgearbeitet werden.

Grundsätzlich »hängen« die Rechte, was wer mit einem Objekt/einer Ressource tun darf, am Objekt selber. Objekte sind Laufwerke, Verzeichnisse, Dateien oder Drucker, aber auch die Registry (Abschnitt 2.8). Nur lokale Gruppen (Abschnitt 2.3.4) erhalten Rechte an Objekten auf einem Domänen-Rechner. Globale Gruppen bekommen Rechte, indem sie Mitglied einer lokalen Gruppe werden. Bei zentraler Administration geht die Übersicht bezüglich der Rechtevergabe leicht verloren.

Die Interessenvertretung sollte sich die Organisation und Arbeitsteilung in der Administration genau ansehen. Ein nachvollziehbares formales Freigabeverfahren für die Erteilung von Benutzerkonten und Rechten sollte in jedem Fall dann eingerichtet werden, wenn personenbezogene Daten der Mitarbeiter verarbeitet werden.

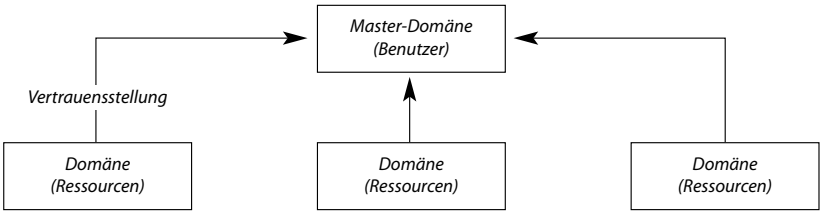


Abbildung 4: Master-Domänen-Modell

Die Multiple-Master-Domäne

Große Netzwerke lassen sich in der vorstehend beschriebenen Art schwer verwalten. Für diese Situation empfiehlt Microsoft, mehrere Master-Domänen einzurichten. Dieses Modell wird als Multiple-Master-Domäne bezeichnet. Ebenso wie im Master-Domänen-Modell bringt auch hier jede sekundäre oder Ressourcen-Domäne jeder Master-Domäne eine einseitige Vertrauensstellung entgegen. Die Master-Domänen vertrauen sich wechselseitig. So braucht ein Benutzer im gesamten Netzwerk nur einmal eingerichtet und administriert zu werden, wobei die Administration in diesem Fall von den Administratoren jeder Master-Domäne wechselseitig erfolgen kann.

Der Administrations- und Koordinationsaufwand in der Benutzerverwaltung ist erheblich, da zumindest die globalen Gruppen zwischen den Master-Domänen abgestimmt sein müssen. Die oben angeführten Anmerkungen zur Sicherheitsproblematik treffen auch hier zu.

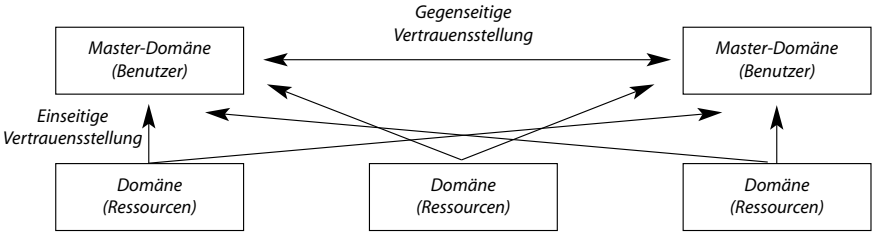


Abbildung 5: Multiple-Master-Domänen-Modell

Complete-Trust-Modell

Das vierte Modell ist der Vertrauensverbund (Complete-Trust-Modell). In diesem Modell bringen sich alle Domänen eine gegenseitige Vertrauensstellung entgegen. Da jede Domäne Benutzer anlegen kann, die wiederum in den anderen Domänen akzeptiert werden, ist der Vorteil der möglichst zentralen Benutzerverwaltung nicht gegeben.

Die Sicherheit im Multiple-Master-Domänen-Modell ist nur mit großem Aufwand sicherzustellen, da hier ein extrem hoher Koordinationsbedarf bei den gegenseitigen Freigaben, Benutzer- und Gruppenbezeichnungen notwendig ist.

2.4 BENUTZER- UND GRUPPENVERWALTUNG

2.4.1 Benutzerverwaltung

Die Einrichtung von Benutzern und Gruppen kann mit Hilfe des von Windows NT bereitgestellten graphischen Verwaltungsprogramms, dem Benutzermanager für Domänen (am PDC) oder dem Benutzermanager (an der Workstation) sowie direkt auf der Kommandozeile der Eingabeaufforderung erfolgen.

Die Benutzer- und Gruppenverwaltung muß nicht direkt am Server erfolgen! Da der physische Zugriff auf den Server in der Regel ein Sicherheitsrisiko darstellt, erhalten die Administratoren die Möglichkeit, an ihrem Arbeitsplatz die Administrationsaufgaben wahrzunehmen. Dazu ist wie schon oben erwähnt die Installation des »Benutzer Manager für Domänen« auf dem Arbeitsplatzrechner des Administrators notwendig. Um weitere Benutzer anzulegen und zu verwalten, kann über das Menü

START ➡ PROGRAMME ➡ VERWALTUNG (ALLGEMEIN) ➡ BENUTZER-MANAGER

das graphische Benutzerverwaltungsprogramm aufgerufen werden. Alle standardmäßig auf der Installations-CD mitgelieferten Programme befinden sich im Verzeichnis WINNT. In der Regel – Umbenennung ist möglich – liegen die Verwaltungsprogramme im Verzeichnis WINNT\system32.

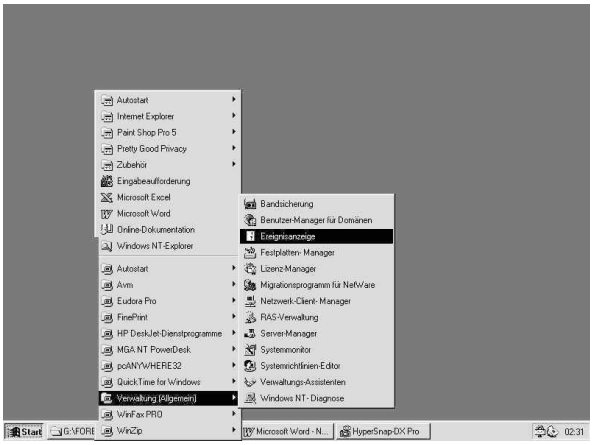


Abbildung 6: »Menüweg« zu den Verwaltungsprogrammen

Wer auf das Verzeichnis WINNT in welchem Umfang Zugriffsrechte hat, sollte geprüft werden. Standardmäßig ist Windows NT in seiner Rechtevergabe bei der Installation sehr offen und benötigt für eine halbwegs sichere Einrichtung eine »Nachbesserung«.

Zahlreiche Programme zur Verwaltung von NT und auch die mächtigen Werkzeuge zur Bearbeitung der Registry regedt32.exe und regedit.exe stehen der Gruppe JEDER und NETZWERK und damit allen Domänenbenutzern offen. Berechtigungen »vererben« sich. Die Gruppe JEDER hat standardmäßig das Recht »VOLLZUGRIFF« auf der obersten Ebene des Rechners bzw. des Laufwerks, also die Laufwerke C:\ oder D:\ .

Entzug des Rechts VOLLZUGRIFF für die Gruppe JEDER. Anschließend differenzierte Neuzuweisung von Rechten an Objekten für die Gruppe JEDER.

Die auf dem Benutzermanager für Domänen zur Verfügung stehenden Möglichkeiten der Benutzerverwaltung unterscheiden sich vom Benutzermanager auf der Workstation in den serverspezifischen Funktionen.

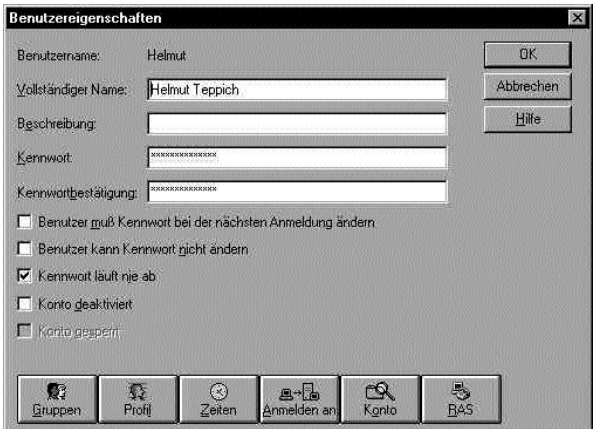


Abbildung 7: Benutzer anlegen auf dem Server

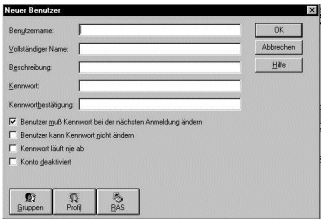


Abbildung 8: Benutzer anlegen auf der Workstation

Vordefiniert, d. h. bei der Installation automatisch angelegt, sind die beiden Benutzer »Administrator« und »Gast«. Die Festlegung neuer Benutzer erfolgt über das Eröffnungsfenster des Benutzermanagers, in dem mindestens der Name des Benutzers für die Anmeldung anzugeben ist.

Für eine sichere Benutzerumgebung darf von den vier linken Kästchen bei der Anlage eines neuen Benutzerkontos nur das erste »Benutzer muß Kennwort bei der nächsten Anmeldung ändern« aktiviert sein.

GRUPPEN: In beiden NT-Typen – Workstation wie Server – können Gruppen Benutzer zugeordnet werden, wodurch sie die für diese Gruppen festgelegten Rechte zugewiesen bekommen. Benutzer können auch in mehreren Gruppen gleichzeitig Mitglied sein. Unterscheiden sich die Rechte der Gruppen an einer Ressource (z. B. einem Verzeichnis), bei denen ein Benutzer Mitglied ist, werden für den betreffenden Benutzer die Rechte seiner Gruppen addiert. Ausgenommen davon ist die Situation, in der einer Gruppe explizit das Recht »Kein Zugriff« zugewiesen wurde. »Kein Zugriff« ist ein Veto, d. h. dieses Recht überlagert alle anderen Rechte.

Abbildung 9: Gruppenzuordnung

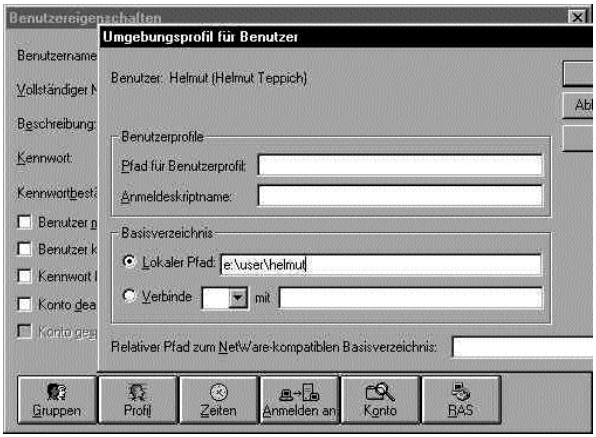


Abbildung 10: Umgebungsprofile

PROFIL: Mit dem Schalter »Profil« werden Vorgaben für Benutzerverzeichnisse, Anmeldeskripte und Anmeldeprogramme gesetzt. Aus der Einstellung ist hier erkennbar (weil nichts eingetragen ist), daß es sich um ein lokales Profil auf dem Rechner handelt. Unter WINNT\Profiles sind auf dem lokalen Rechner die Informationen abgelegt, die bei der Anmeldung abgefragt werden.

ZEITEN: Mit dem Schalter »Zeiten« lassen sich Zeiträume definieren, zu denen der Zugang zum System zulässig bzw. unzulässig ist. Dieser Schalter wird nach unserer Erfahrung selten genutzt, obwohl sich hier z. B. auch Arbeitszeitvereinbarungen direkt umsetzen lassen. Als Argument gegen eine Nutzung in Form von Zeitvorgaben wird hier meist der hohe Pflegeaufwand angegeben. Unter der Hand wird aber auch zugegeben, daß dadurch die gewünschte Flexibilität in der Arbeitszeit unterbunden wird.

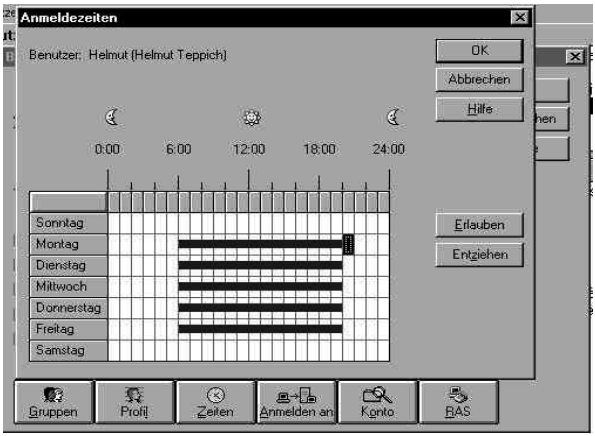


Abbildung 11: Anmeldezeiten

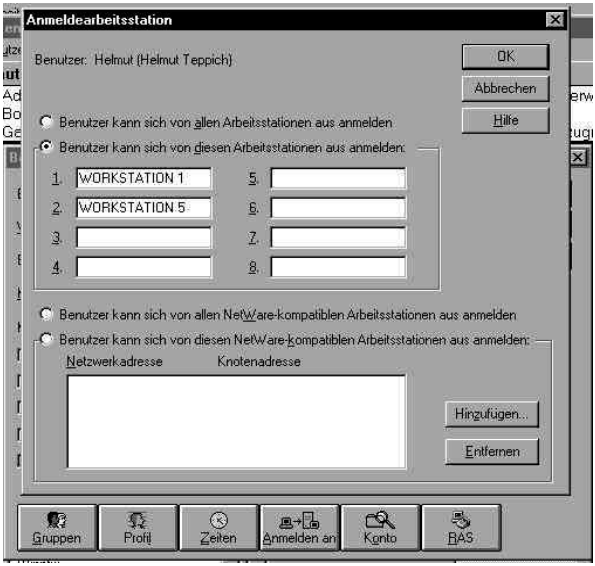


Abbildung 12: Anmelden an

ANMELDEN AN: Ähnliches – in bezug auf die praktische Relevanz – trifft nach unserer Erfahrung auf die Vorgabe der Rechner unter dem Schalter »Anmelden an« zu. Insbesondere Benutzer mit Zugang zu sensiblen Daten (z. B. in der Personalverwaltung) können mit dieser Einstellmöglichkeit auf bestimmte Arbeitsplätze festgelegt werden. Sich mal schnell irgendwo im Betrieb am System anzumelden und dort Daten anzusehen oder zu verarbeiten, würde damit verhindert werden.

KONTO: Mit den Kontenvorgaben können Vorgaben für die Gültigkeitsdauer eines Benutzerkontos gemacht werden, z. B. zur Vermeidung von »Kontenfriedhöfen« und zur regelmäßigen Kontrolle und Korrektur der angelegten Daten.

Das Setzen eines Gültigkeitsendes, z. B. bei Aushilfskräften, bei externen Beratern oder Mitarbeitern mit Zeitverträgen, wird unseres Erachtens oft aus Bequemlichkeit nicht genutzt.

Das Argument des hohen Pflegeaufwands ist unserer Meinung nach vorgeschoben, denn gepflegt werden muß ja nur, wenn die Person über das gesetzte Limit hinaus tätig bleibt. In einem solchen Fall sind aber diverse Stellen im Unternehmen (z. B. Personal) ohnehin mit Vertragsanpassungen befaßt. Eine formale Kommunikation zur Einrichtung von Benutzerkonten müßte für den Alltagsbetrieb zwischen Personalverwaltung und NT-Administration eigentlich existieren und wäre hier gefragt. Die Gefahr, daß Benutzern Zugriffsrechte auf sensible Daten (egal welcher Art) über ihr Vertragsende hinaus zur Verfügung stehen und genutzt werden, ist nicht zu unterschätzen. Vor allem in Domänen mit Hunderten von Benutzern geht die Übersicht schnell verloren. Die Problematik gilt oft noch mehr für Personen, die innerhalb des Unternehmens eine andere Tätigkeit aufnehmen, in der Domäne aber ihr altes Konto und damit ihre alten Rechte behalten. Da NT jedem Benutzer eine interne einmalige SID (Security ID) vergibt, können Benutzerkonten gelöscht und neue unter gleichem Namen wieder eröffnet werden. Für den scheinbar gleichen Benutzer sind die alten Rechte nicht mehr verfügbar, da er eine andere SID bekommen hat. Der bloße Wechsel einer Gruppenmitgliedschaft reicht unseres Erachtens nicht aus, denn oft erhalten Benutzer über ihre Gruppenmitgliedschaft hinaus weitere Rechte, z. B. auf ihrem lokalen Rechner, aber auch auf dem Server, den sie allerdings oft nicht an den neuen Arbeitsplatz mitnehmen.

Windows NT ermöglicht es nicht, für einen bestimmten Benutzer festzustellen, welche Rechte er an welchen Objekten hat.

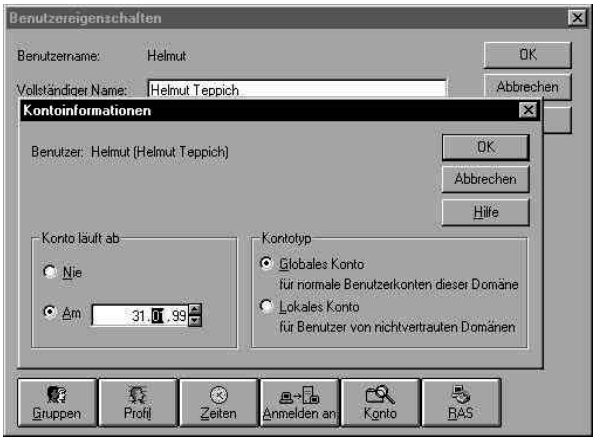


Abbildung 13: Kontovorgaben

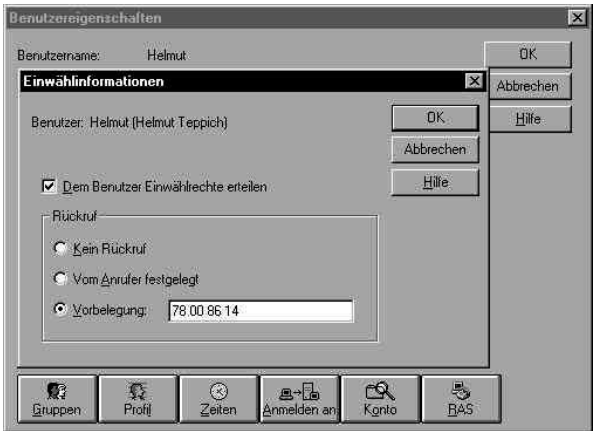


Abbildung 14: RAS-Einwählvorgaben

RAS: Das Recht des RAS (Remote Access Service)-Zugriffs autorisiert den Benutzer, sich über eine Modem/ISDN-Verbindung von außerhalb der Domäne (z. B. von unterwegs, von zu Hause, von der Beraterfirma, …) einzuwählen und die freigegebenen Ressourcen zu nutzen bzw. nach außen zu kommunizieren.

Im Zusammenhang mit der Vorgabe der zulässigen Anmeldezeiten werden hier Möglichkeiten geschaffen, von zu Hause oder unterwegs auf den Betriebsrechner und die freigegebenen Ressourcen zuzugreifen. Unabhängig von der Problematik »Arbeitszeit« spielt es hier eine Rolle, auf welche Art von Daten von Benutzern mit RAS-Berechtigung zugegriffen werden darf.

Für Benutzer aus Personalverwaltung und Personalwirtschaft dürften nach unserer Meinung RAS-Berechtigungen nicht vergeben werden, da der Weg der Daten bei einem solchen Zugriffsrecht nicht mehr nachvollziehbar wäre.

Ausgeschiedenen Mitarbeitern mit RAS-Berechtigung steht der Zugriff auf die alten Daten offen, wenn ihr Konto nicht gesperrt wurde.

Unabhängig von der generellen Problematik des Fernzugriffs ist nur die Einstellung mit Rückwahl insofern sicher, als zumindest der Gegenanschluß bekannt ist. Die anderen beiden Varianten setzen von seiten des Betriebes großes Vertrauen voraus, denn von wo betriebsinterne Daten eingesehen und gegebenenfalls auch kopiert werden, ist allein Sache des Anrufers.

2.4.2 Benutzerverwaltung mit Befehlseingabe

Für die Administration in kleinen Netzen mag die Anwendung des graphischen Benutzermanagers praktikabel sein. Administratoren von großen Netzen richten Hunderte von Benutzern aber nicht einzeln mit den graphischen Verwaltungsprogrammen, sondern mit Kommandozeilenprogrammen, wie z. B. dem Befehl »net user« oder dem Programm »adduser« (Bestandteil des sog. Windows NT Ressource Kit = Technische Referenz) ein. Die Benutzung der Kommandozeilenprogramme umgeht nicht das Protokollieren von Aktivitäten, sofern eine Überwachung bestimmter Ereignisse eingestellt wurde (siehe Abschnitt 2.5.3).

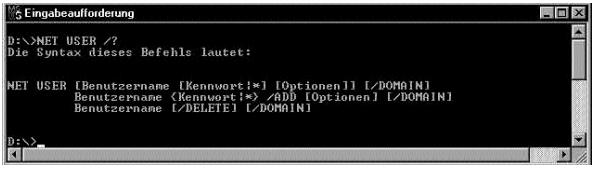


Abbildung 15: Benutzer anlegen mit NET USER

Abbildung 16: Benutzer »Samson« angelegt

Unabhängig von der Vorliebe für eine bestimmte Benutzeroberfläche besteht bei beiden Varianten der Benutzerverwaltung die Möglichkeit, Muster-Benutzer anzulegen, die dann im Bedarfsfall »nur« mit den spezifischen Daten angepaßt werden müssen.

Durch Nutzung von Scripten ist dies mit den Kommandozeilenprogrammen erheblich schneller möglich, als bei Festlegung von Hand.

Problematisch ist die Möglichkeit, unbenutzte Benutzerkonten auf Vorrat anzulegen. Die Anlage von unbenutzten Konten, z. B. ABC 100 bis ABC 200, die dann von Personen, die nicht zur Administration gehören (z. B. Vorgesetzte), an konkrete Personen »vergeben« werden, birgt erhebliche Gefahren.

Dieser Praxis sollte nicht zugestimmt werden. Technisch zu unterbinden ist diese Vorgehensweise allerdings nach unserer Erfahrung nicht. Sind Vorgesetzten solche Vorratskonten bekanntgegeben worden, werden sie die auch »verteilen«. Sicher ist die Zuweisung von Konten an Mitarbeiter in jedem Einzelfall entsprechend einem formalen Freigabeverfahren.

2.4.3 Gruppen

Windows NT unterscheidet in seinem Organisationskonzept zwischen globalen und lokalen Gruppen:

Globale Gruppen können ausschließlich auf dem PDC definiert werden. Sie dienen dazu, Benutzer domänenweit organisatorisch zusammenzufassen und die Strukturen des Betriebes/Unternehmens auf der EDV abzubilden. Globale Gruppen werden i.d.R. zu Mitgliedern in lokalen Gruppen der einzelnen Rechner der Domäne gemacht, um ihren Mitgliedern Rechte auf dessen Ressourcen zu verschaffen. Nur Domänenbenutzer können Mitglieder einer globalen Gruppe werden, andere Gruppen können nicht Mitglied in einer globalen Gruppe werden.

Lokale Gruppen werden auf einzelnen Rechnern (dies gilt auch für den PDC selbst) definiert. Sowohl Benutzer wie auch globale Gruppen können Mitglied einer lokalen Gruppe werden. Andere lokale Gruppen können nicht Mitglied einer lokalen Gruppe werden. Lokale Gruppen haben die Funktion, ihren Mitgliedern Rechte an Ressourcen (Laufwerken, Verzeichnissen, Dateien, Druckern) auf dem einzelnen Rechner zuzuweisen. Die einzelnen Mitglieder einer lokalen Gruppe können auch aus verschiedenen Domänen stammen, falls zwischen den Domänen Vertrauensbeziehungen bestehen.

Das »Verhältnis« von den beiden Gruppentypen und ihren Rechten verläuft grundsätzlich:

- Domänenbenutzer werden Mitglieder in globalen Gruppen
- Globale Gruppen werden Mitglieder in lokalen Gruppen

- Lokale Gruppen bekommen Rechte an Ressourcen zugewiesen
- Ressourcen sind die Träger ihrer Rechte

Die Festlegung von Gruppen und Gruppenmitgliedschaften wird – sofern nicht mit der Eingabeaufforderung oder einem Kommandozeilenprogramm gearbeitet wird – mit dem Benutzermanager durchgeführt. Die entsprechenden Benutzer und Gruppen stellen sich mit diesen Icons dar:

 lokaler Benutzer

 lokale Gruppe

 globaler Benutzer

 globale Gruppe

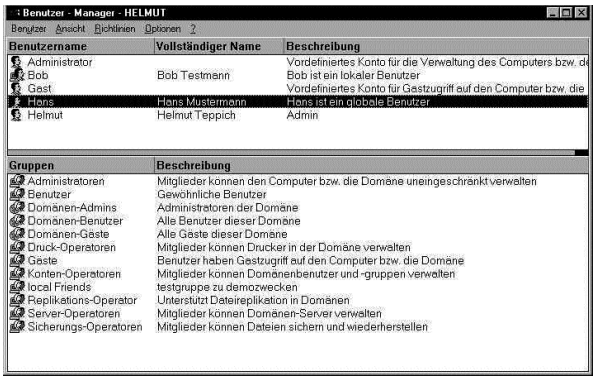


Abbildung 17: Benutzer und Gruppen auf dem Server

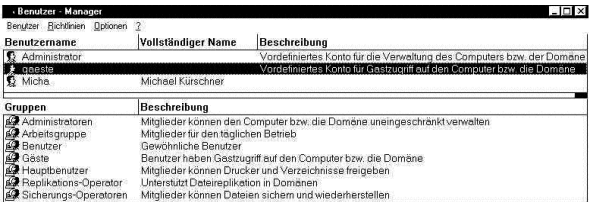


Abbildung 18: Benutzer und Gruppen auf der Workstation

Vordefinierte Gruppen

Nach der Installation von Windows NT sind abhängig vom Systemtyp (PDC, Server oder Workstation) Gruppen mit vordefinierten bestimmten Rechten eingerichtet. Die vom System vordefinierten Gruppen unterteilen sich in lokale (Server und Workstation) und globale (PDC) Gruppen.

Lokale Gruppen auf der Workstation

Administratoren	Mitglieder dieser Gruppe haben Administrationsrechte auf dem lokalen Rechner.
Gäste	Mitglieder dieser Gruppe haben Gast-Zugriffsberechtigung mit begrenzten Zugriffsrechten. Auf Domänen-Controllern ist diese Gruppe bei der Installation deaktiviert.
Benutzer	Mitglieder dieser Gruppe sind alle Benutzer des Systems. Bei der Installation wird ihr auf dem Server die Gruppe der Domänen-Benutzer als Mitglied zugewiesen.
Sicherungs-Operatoren	Mitglieder dieser Gruppe haben das Recht, Dateien zu sichern und wiederherzustellen, auch wenn sie sonst keinerlei Zugriffsrechte auf Dateien haben.
Replikations-Operatoren	Mitglieder dieser Gruppe sind für die Replikation zwischen NT-Servern zuständig.
Hauptbenutzer (PowerUser)	Diese Gruppe ist nur auf der Workstation vordefiniert. Mitglieder dieser Gruppe haben weitgehende Rechte zur Verwaltung und Administration einer Workstation.

Hauptbenutzer haben auf einer Workstation administratorähnliche Rechte. Wer auf welcher Workstation dieses Recht erhält, sollte von der Interessenvertretung mitbestimmt werden.

(Zusätzliche) Lokale Gruppen auf Servern und Domänen-Controllern

Server-Operatoren	Mitglieder dieser Gruppe haben das Recht, alle Domänen-Controller zu verwalten.
Konten-Operatoren	Mitglieder dieser Gruppe haben das Recht, die Benutzerkonten der Domäne zu verwalten (ausgenommen davon sind die Administrationskonten). Sie können keine Benutzerrechte vergeben, kein Auditing verwalten und keine Kontenregeln ändern.
Druck-Operatoren	Mitglieder dieser Gruppe haben das Recht, alle Drucker zu verwalten.

Globale Gruppen auf Domänen-Controllern

Domänen-Administratoren	Mitglieder dieser Gruppe haben uneingeschränkte Rechte in einer Domäne. Der Administrator des PDC ist automatisch Mitglied dieser Gruppe. Die Gruppe ist Mitglied der lokalen Administrations-Gruppe auf dem PDC.
Domänen-Gäste	Mitglieder dieser Gruppe haben Gast-Zugriffsberechtigung mit begrenzten Zugriffsrechten. Die Gruppe ist Mitglied der lokalen Gast-Gruppe auf dem PDC.
Domänen-Benutzer	Alle Benutzer einer Domäne sind automatisch Mitglied dieser Gruppe. Die Gruppe ist Mitglied der lokalen Benutzer-Gruppe auf dem PDC.

Zusätzlich zu den im Benutzermanager aufgelisteten Gruppen gibt es Gruppen, die nicht ausdrücklich definiert werden und erst bei der Vergabe von Zugriffsrechten »auftauchen«:

JEDER	Ist jeder Benutzer des Rechners, eine Kombination aus den Gruppen INTERAKTIV und NETZWERK.
INTERAKTIV	Alle Benutzer, die lokal am Rechner arbeiten können.
NETZWERK	Alle Benutzer, die über ein Netzwerk mit dem Rechner arbeiten.
ERSTELLER-BESITZER	Alle Benutzer, die ein Verzeichnis, ein Unterverzeichnis, eine Datei, einen Drucker oder ein Dokument, das zu einem Drucker gesandt wird, erstellt oder das Recht des Besitzes übernommen haben.
SYSTEM	Das Betriebssystem

Bereits mit den vordefinierten Gruppen kann ein minimales Sicherheitskonzept erstellt werden, in dem z. B. die Berechtigung »Administrator« bzw. »Domänen-Administrator« nach Einrichtung der Sub-Administratoren per 4- oder Mehr-Augen-Prinzip gesperrt und weggeschlossen wird und die Administration »nur noch« über die Sub-Administratoren erfolgt.

Die Möglichkeit, Administrationsaufgaben zu verteilen und damit auch eine höhere Sicherheit zu erreichen, wird in vielen NT-Installationen nicht realisiert. Mit der Begründung des hohen Kostenaufwandes und dem Vertrauen in die Administratoren (Vor-

wurfsvolle Frage an die Interessenvertretung: Warum haben Sie eigentlich kein Vertrauen zu unseren Administratoren?) bleiben die Sub-Administratorenkonten oft ungenutzt.

2.4.4 Globale Gruppen

Die Definition von globalen Gruppen kann nur für eine Domäne stattfinden. Die Festlegung von globalen Gruppen dient der Strukturierung aller Domänenbenutzer. Globale Gruppen können z. B. die organisatorische Struktur eines Unternehmens widerspiegeln, in dem die Gruppen nach Standorten eingeteilt werden. Globale Gruppen können auch nach temporären Strukturen innerhalb einer Organisation definiert werden, z. B. nach zeitlich begrenzten Projekten. Durch Zuweisung der Mitgliedschaft einer globalen Gruppe »Projekt A« in der lokalen Gruppe eines NT-Rechners erhalten dann die aus unterschiedlichen Standorten stammenden Mitglieder der globalen Gruppe »Projekt A« identische Zugriffsrechte auf bestimmte Ressourcen des NT-Rechners. Ein anderer Strukturierungstyp von globalen Gruppen ist die Unterteilung nach ihrer Rolle in der Organisation. Hier werden die Gruppen nach ihren Tätigkeiten oder Einsatzgebieten gebildet. Beispiele dafür wären: Datenbank-Administratoren, SAP-Benutzer, SAP-Administratoren oder Internet-Benutzer.

Wird bei der Zuordnung von Benutzern zu globalen Gruppen bzw. von globalen Gruppen zu lokalen Gruppen auf das 4-Augen-Prinzip oder ein anderes verbindliches Freigabeverfahren verzichtet, können sich Sicherheitslücken ergeben. Dies ist vor allem bei großen Domänen und Domänen mit Vertrauensstellungen möglich. Aber auch in kleinen Betrieben, in denen nur wenige oder sogar nur eine einzige Person als allumfassender Administrator fungiert, bleiben durch die Komplexität der Benutzerverwaltung Schutzrechte und Sicherheitsüberlegungen auf der Strecke.

2.5 WEITERE WICHTIGE FUNKTIONEN IM BENUTZERMANAGER

Neben der Aufgabe der Benutzer- und Gruppenverwaltung dient der Benutzermanager im PDC auch zur Aktivierung und Einstellung allgemeiner, rechnerweiter Richtlinien. Dazu zählen die Richtlinien für Konten, die Benutzerrechte und die Aktivierung der Überwachung.

An jedem Server und jeder Workstation erhält man (sofern dazu berechtigt) über die Menüfolge START ➡ Programme ➡ Verwaltung (allgemein) ➡ Benutzer-Manager den notwendigen Zugang zur Benutzerverwaltung. Im Menü BENUTZER kann der Administrator unter dem Menüpunkt »Domäne auswählen« auf die Benutzerverwaltung eines jeden Rechners in der Domäne zugreifen.

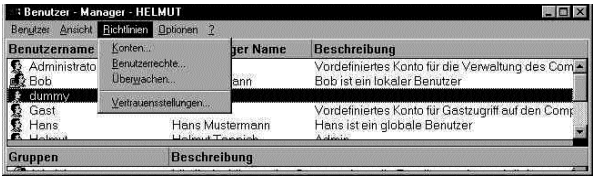


Abbildung 19: Richtlinienmenü im Benutzermanager (Server und Workstation)

Nur soweit die Ereignisprotokolle auf einem Rechner bereits aktiviert wurden, werden hier vorgenommene Änderungen protokolliert.

Die Ereignisprotokollierung sollte immer – bis auf die Prozeßverfolgung – für beide Erfolgsvarianten aktiviert werden. Soweit dann die Datei- und Verzeichnisprotokollierung noch nicht für konkrete Objekte aktiviert wurden, beschränkt sich die Protokollierung auf die Tätigkeiten der Administratoren.

2.5.1 Richtlinien für Konten

In diesem Fenster werden die Richtlinien für Kennwörter und das Verhalten von NT im Fall eines unberechtigten oder fehlerhaften Zugriffsversuchs festgelegt.

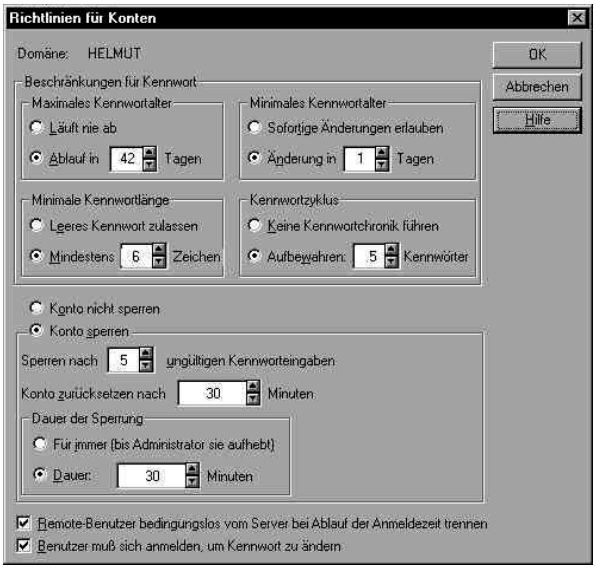


Abbildung 20: Richtlinien für Konten (auf dem Server)

Die Einstellungen der Kontenrichtlinien gelten nur für die auf dem jeweiligen Rechner verwalteten Konten.

Handelt es sich um einen primären Domänen-Controller, der alle Domänen-Benutzer verwaltet, gelten die Richtlinien für alle Domänen-Benutzer. Bei der Prüfung eines NT-Systems sollten die Einstellungen in diesem Fenster immer geprüft werden (siehe Abschnitt 8.4). Die Kontosperrung unten links wird – wieder aus »Praktikabilitätsgründen« – oft nicht aktiviert, wodurch unbegrenzte Anmeldeversuche möglich werden. Beliebige Anmeldeversuche sind dann auch über einen Fernzugriff per Modem/ISDN möglich, sofern der Benutzer eine RAS-Berechtigung hat.

Wurden im Menü »Anmeldezeiten« Arbeitszeiten vorgegeben und das Kästchen »Remote Benutzer« aktiviert, wird der betreffende Benutzer zum Ende der eingerichteten Arbeitszeit von der Domäne getrennt. Die Trennung erfolgt nur bei Zugriff über eine Remote- oder RAS-Verbindung. Sitzt der Benutzer am Arbeitsplatz, wird er nicht getrennt. Nur im Fall der Abmeldung kann er sich dann nicht wieder an der Domäne

anmelden. Wohl aber an seinem Arbeitsplatzrechner, sofern auf diesem keine Arbeitszeit vorgegeben ist (NT) oder nicht vorgegeben werden kann (W95).

Der Zwang, nur in angemeldetem Zustand ein neues Paßwort festlegen zu können, führt bei abgelaufenen Konten und Paßwörtern dazu, daß nur die Administratoren den Zugang wieder öffnen können. Die beiden Kästchen sollten deshalb aktiviert sein.

2.5.2 Richtlinien für Benutzerrechte

Den Benutzern oder Gruppen werden 27 Benutzerrechte zugewiesen. Sie erlauben den bei dem einzelnen Recht eingetragenen Benutzer bzw. der Gruppe, bestimmte Aktionen am NT-Rechner durchzuführen. Zu beachten ist, daß die integrierten Systemrechte nichts mit den Freigaben oder den Berechtigungen für eine Ressource zu tun haben. Freigaben oder Berechtigungen sind Rechte an Ressourcen und werden für die konkrete Ressource (Laufwerk, Verzeichnis, Datei, Drucker, Registry) vergeben.

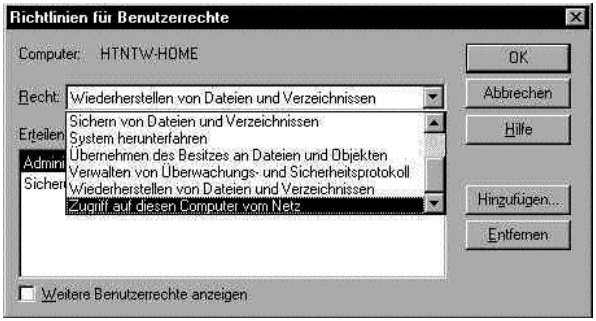


Abbildung 21: Richtlinien für Benutzerrechte (auf der Workstation)

Interessant für die Interessenvertretung ist z. B. das Benutzerrecht »Verwaltung von Überwachungs- und Sicherheitsprotokoll«.

In der Installation wird das Recht der Protokollverwaltung dem Administrator gegeben. Um auch Aktivitäten der Administratoren überwachen zu können, wird empfohlen, dieses Recht einer speziellen Gruppe, z. B. der Gruppe »REVISION«, zu geben und es den Administratoren zu entziehen.

Dafür muß eine globale Gruppe REVISION und auf den entsprechenden Rechnern eine lokale Gruppe REVISION angelegt werden. Mitglieder in der Revisionsgruppe könnten z. B. die Interessenvertretung, EDV-Revisoren und der Datenschutzbeauftragte sein.

Durch den Entzug des Benutzerrechts »Verwaltung von Überwachungs- und Sicherheitsprotokoll« haben die Administratoren dennoch die Möglichkeit, die Ereignisprotokolle einzusehen, sie sind in ihrer Arbeit also nicht behindert. Wurden Sub-Administratoren anstelle des ursprünglichen Administrators eingerichtet, besteht für sie keine Möglichkeit, sich dieses Recht wieder zuzuweisen, da sie keinen Zugriff auf diesen Menüpunkt haben. Mitglieder der Gruppe »Administratoren« können dies, allerdings wird diese Richtlinienänderung im Sicherheitsprotokoll unter der Ereignisnummer 608 (zuweisen) bzw. 609 (entfernen) festgehalten.

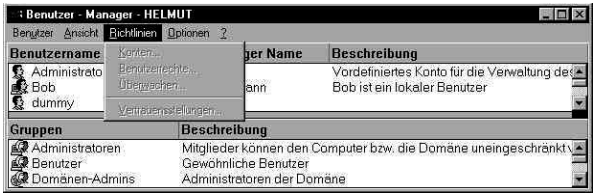


Abbildung 22: Kontenadministrator hat kein Zugriff auf Richtlinien

2.5.3 Überwachungsrichtlinien

Unter dem Menüpunkt »Überwachen« wird zum einen die Überwachung grundsätzlich aktiviert. Zum anderen wird festgelegt, welche konkreten Ereignisse durch die Ereignisprotokolle »System«, »Sicherheit« und »Anwendung« überwacht werden sollen.

Die Aktivierung der Überwachung beschränkt sich auf den einzelnen Rechner. An einem überwachten PDC werden also nur die Anmeldung und die Aktivitäten auf dem PDC protokolliert. Die Zugriffe auf andere Rechner der Domäne werden gegebenenfalls auf den anderen Rechnern festgehalten.

Müssen mehrere NT-Rechner überwacht werden, ist die Protokollierung also auf jedem einzelnen Rechner neu zu aktivieren, damit die zu schützenden Ressourcen (Laufwerke, Verzeichnisse, Dateien, Drucker, …) überwacht werden.

Die Nutzung der Überwachung setzt zwingend voraus, daß die zu überwachenden Objekte sich auf einem Laufwerk mit dem Dateisystem NTFS befinden. Damit scheiden alle FAT-formatierten Laufwerke für die Überwachung, wie sie bei Windows 95 oder 98 üblich sind, aus!

Abbildung 23: Überwachungsrichtlinien

Das Aktivieren der Überwachung wirkt sich sofort aus. Nur für die Datei- und Objektzugriffe entstehen noch keine Überwachungseinträge, da die Überwachung immer konkret am zu überwachenden Objekt aktiviert werden muß.

Die Aktivierung der Überwachung führt nach unseren Erfahrungen ohne Prozeßverfolgung und ohne Objektüberwachung zu keiner Verlangsamung eines Systems (sofern dieses nicht sowieso schon an der Kapazitätsgrenze arbeitet).

Die Aktivierung der Prozeßverfolgung ist für die Interessenvertretung unwichtig, sie dient der technischen Administration und wird nur kurzfristig erfolgen, da die Prozesse enorme Datenmengen produzieren, die die Ereignisprotokolle innerhalb kürzester Zeit vollschreiben.

Zur Einsichtnahme und Verwaltung der Ereignisprotokolle dient standardmäßig die Ereignisanzeige, eines der Verwaltungsprogramme, das unter dem Menü START ➡ Programme ➡ Verwaltung (allgemein) aufgerufen werden kann.

NT hat drei Protokollarten in der Ereignisanzeige vereint: das Sicherheitsprotokoll, das Systemprotokoll und das Anwendungsprotokoll. Größe und Speicherdauer lassen sich differenziert für jedes Protokoll einstellen.

Nur wenn die Größe des Protokolls nicht auf Null steht, werden Einträge in das jeweilige Protokoll vorgenommen. Die Einstellung erfolgt in der Ereignisanzeige unter EREIGNISANZEIGE ➡ Protokoll ➡ Protokolleinstellungen.

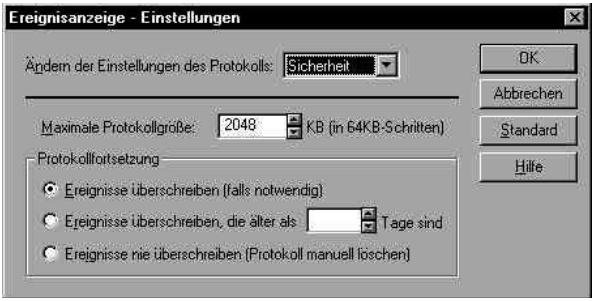


Abbildung 24: Einstellungen Ereignisprotokoll

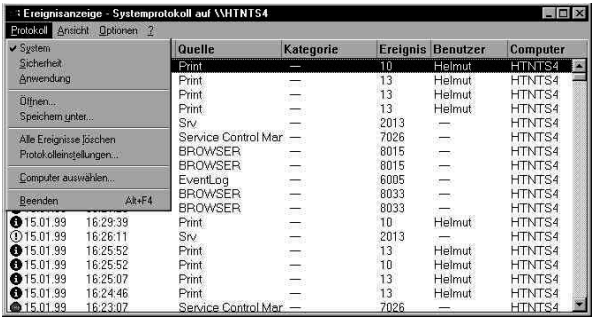


Abbildung 25: Einstellungen der Ereignisprotokolle

Die Protokolle werden unter den Dateinamen SecEvent.Evt, SysEvent.Evt und AppEvent.Evt standardmäßig im Verzeichnis WINNT\system32\config gespeichert. Soweit die Dateien dort nicht zu finden sind, lassen sie sich mit dem systemweiten Suchbefehl aufspüren. Unter START ➡ SUCHEN ➡ DATEI/ORDNER ➡ Name = »*.evt« lassen sich die Dateien am schnellsten finden. Im Fall der Umbenennung – dies ist nur durch die Administratoren möglich – gibt die Registry unter HKEY_LOCAL_MACHINE\System\ CurrentControlSet\ Services\EventLog Auskunft, wo die Dateien gespeichert werden und wie sie jetzt heißen.

Die Detailinformationen der einzelnen Ereignisse sind mehr oder weniger aussagefähig. Ohne zusätzliche Literatur oder die Nutzung der Hilfsdateien bleiben die Informationen in der Regel kryptisch. Dies ist eine oft bemängelte Schwäche von Windows NT.

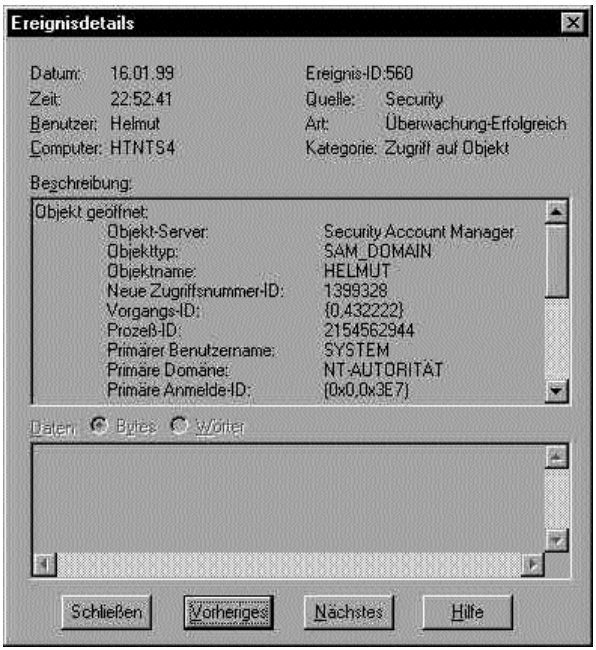


Abbildung 26: Ereignisdetailanzeige

Auch die Anzeige mit der Ereignisanzeige ist umständlich und zeitaufwendig. Dementsprechend haben sich Produkte von Drittanbietern dieses Bedürfnisses angenommen und deutlich bessere Lösungen für die Auswertung und auch Archivierung der Protokolle entwickelt.

Abbildung 27: Ereignisdetailanzeige mit ELWIZ

2.6 FREIGABEN

Sollen Laufwerke oder Verzeichnisse im Netzwerk für andere Teilnehmer in irgendeiner Weise nutzbar sein, so müssen sie freigegeben sein. Erst die Freigabe führt dazu, daß die freigegebenen Laufwerke oder Verzeichnisse im Netzwerk angezeigt werden. Dateien lassen sich nicht freigeben, ihr Schutz hängt an den sie umfassenden Verzeichnissen. Das Prinzip der Freigabe im Netzwerk gab es schon unter Windows for Workgroups. Für die Freigabe bei NT kann eine beliebige, bis zu 80 Zeichen lange Bezeichnung gewählt werden. NT erstellt bei der Installation standardmäßig auch sogenannte versteckte Freigaben. Dabei handelt es sich um alle Laufwerke sowie um Freigaben für die Administration und die Anmeldung. Versteckte Freigaben (sie enthalten alle das Zeichen $ am Ende , z. B. C$) sind im Windows NT Explorer nicht zu erkennen. Sie lassen sich aber bei Kenntnis der Bezeichnung z. B. auf dem Schreibtisch über das Icon »Netzwerkumgebung« und »Netzlaufwerk verbinden« ansprechen. Jede neue Freigabe läßt sich als versteckte Freigabe kennzeichnen.

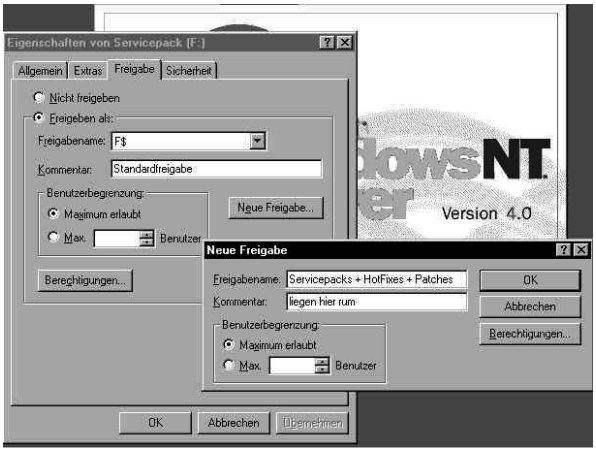


Abbildung 28: Freigabe des Laufwerks F:

Ob und welche versteckten Freigaben es auf einem Rechner gibt, kann im Servermanager, einem weiteren NT-Administrationsprogramm, angezeigt werden.

Bei der Freigabe von Laufwerken oder Verzeichnissen sind folgende Rechte zu vergeben:

Freigabeberechtigung	***Mögliche Optionen für den Benutzer***
Vollzugriff (Standardberechtigung für die Gruppe »Jeder«)	Ändern von Dateiberechtigungen Übernehmen des Besitzes an den Dateien auf NTFS-Datenträgern Ausführen aller bei den Berechtigungen »Ändern« und »Lesen« möglichen Aktionen
Ändern	Erstellen von Ordnern und Hinzufügen von Dateien Ändern von Daten in Dateien Hinzufügen von Daten zu Dateien Ändern der Dateiattribute Löschen von Ordnern und Dateien Ausführen aller bei der Berechtigung »Lesen« möglichen Aktionen
Lesen	Anzeigen der Ordnernamen und Dateinamen Anzeigen von Dateinamen und -attributen Ausführen von Programmdateien Zugreifen auf andere Ordner innerhalb des Ordners
Kein Zugriff	Nur Herstellen einer Verbindung zu dem freigegebenen Ordner Der Zugriff auf den Ordner wird verweigert, und die darin enthaltenen Dateien werden nicht angezeigt. Dieses ist die Berechtigung mit der stärksten Beschränkung, die für eine hohe Sicherheit eingesetzt wird. Die Berechtigung »Kein Zugriff« überschreibt alle anderen Berechtigungen (»VETO«).

Die Icons freigegebener Verzeichnisse (soweit es sich nicht um versteckte Freigaben handelt) sind im NT-Explorer des freigebenden Servers mit einer Hand versehen. Freigaben können nur von Administratoren oder Server-Administratoren eingerichtet werden.

Freigaben können nur für Laufwerke und Verzeichnisse erfolgen. Dateien, die in einem solchen Verzeichnis gespeichert sind, stehen im Rahmen der Freigaberechte zur Verfügung. Nur wenn das Verzeichnis auf einer NTFS-Platte angelegt

wurde, lassen sich bis auf Dateiebene hinab weitere Differenzierungen in den Zugriffsrechten einstellen.

2.7 NTFS UND ZUGRIFFSRECHTE

Windows NT hat ein eigenes Dateisystem: NTFS (New Technology File System). Nur auf NTFS-Laufwerken können die Sicherheitsfunktionen für Objekte (Laufwerke, Verzeichnisse, Dateien, Drucker, Registry) genutzt werden. Ob Festplatten mit NTFS oder FAT-formatiert sind, läßt sich durch den Festplattenmanager, einem der NT-Administrationsprogramme, anzeigen. Der Festplattenmanager liefert auch weitere Detailinformationen über die einzelnen Partitionen.

Für die Realisierung von NT-Systemen, die sensible Daten verarbeiten und die überwacht werden sollen, wird von allen Sicherheitsexperten dringend abgeraten, eine FAT-formatierte Partition auf einem NT-Rechner zu belassen, da hier Angriffsmöglichkeiten bestehen.

Nach unserer Erfahrung wird diese Empfehlung aber erstaunlicherweise oft vernachlässigt. Teilweise wird als Grund angegeben, daß bei ernsthaften Problemen von der FAT-Partition mit DOS-Werkzeugen auf die Daten auf dem NTFS-Laufwerk zugegriffen werden kann. Im Internet existieren dazu entsprechende Angriffs-/Hilfsprogramme. Bei regelmäßiger Datensicherung ist das Risiko des Datenverlustes unseres Erachtens zugunsten der höheren Sicherheit zu vernachlässigen. Sinnvoller wäre es, eine zweite NT-Partition mit einem weiteren NT-System auf dem Rechner zu installieren, so daß man im Falle von Problemen von einem zweiten sicheren System aus auf die Daten zugreifen kann.

NTFS bietet zwar ein höheres Sicherheits- und Überwachungsniveau als z. B. das FAT-Dateisystem, allerdings greift diese Sicherheit nur, wenn der Rechner selbst, dieTastatur und der Monitor physisch gesichert sind.

Wird z. B. eine NTFS-formatierte Platte aus einem Server entfernt und in einem anderen NT-System eingebaut, muß das NT-System (Server oder Workstation) auf dem Rechner nur neu installiert werden. Alle bisher geschützten Ressourcen (im wesentlichen also Dateien) liegen anschließend offen, denn der neue Administrator hat uneingeschränkte Rechte auf dem Server. Die Möglichkeit, sich an einem NT-Server lokal anzumelden,

sollte nur für Ausnahmefälle bestehen. Wer das Benutzerrecht (siehe Abschnitt 2.5.2) »Lokale Anmeldung« hat, sollte bei einer Begehung überprüft werden.

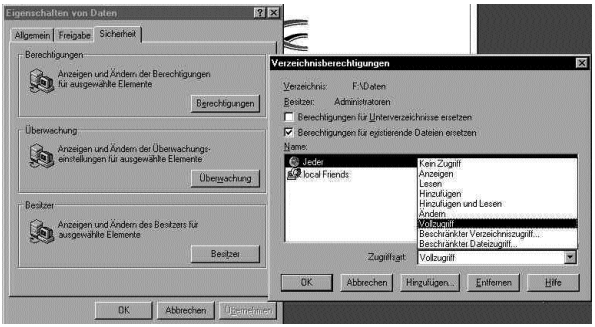


Abbildung 29: NTFS-Berechtigung für F:\Daten zuweisen

Das Dateisystem NTFS ermöglicht, daß über eine differenzierte Vergabe von Zugriffsrechten sich mehrere Benutzer lokal einen NT-Rechner so teilen, ohne auf oder in die Verzeichnisse und Dateien der anderen Benutzer zugreifen zu können.

Die Zugriffsberechtigung auf Verzeichnisse und Dateien läßt sich tief differenzieren. Für einzelne Dateien, wie auch für ganze Verzeichnisse und die in ihnen enthaltenen Dateien, läßt sich festlegen, welcher Benutzer/welche Benutzergruppe welchen Zugriffsumfang haben soll.

Standardmäßig hat die Gruppe JEDER das Recht »Vollzugriff« auf ein Verzeichnis, wenn dieses Zugriffsrecht nach der Installation nicht verändert wird. Für Verzeichnisse mit personenbezogenen Daten darf nie (!) die Gruppe JEDER ein ungeprüftes Zugriffsrecht haben, da diese Gruppe immer alle (!) zugelassenen Benutzer umfaßt und die notwendige Sicherheit und Nachvollziehbarkeit der Datenverarbeitung ohne ein nachvollziehbares Freigabeverfahren nicht gewährleistet ist.

Wird für ein Verzeichnis ein Zugriffsrecht festgelegt, dann vererbt es sich auf alle untergeordneten neuen Verzeichnisse und Dateien, sofern keine anderen Zugriffsrechte festgelegt werden.

Bei Einsatz von NTFS bestehen folgende grundsätzliche Rechte:

NTFS-Berechtigungen	***Ordner***	***Datei***
Lesen (R)	Anzeigen der Namen, Eigenschaften, Besitzer und Berechtigungen eines Ordners	Anzeigen der Namen, Eigenschaften, Besitzer und Berechtigungen einer Datei
Schreiben (W)	Hinzufügen von Dateien und Ordnern, Ändern von Ordnereigenschaften sowie Anzeigen von Besitzer und Berechtigungen	Anzeigen von Besitzer und Berechtigungen, Ändern von Dateieigenschaften, Erstellen von Daten in und Anhängen von Daten an eine Datei
Ausführen (X)	Anzeigen von Ordnereigenschaften, Durchführen von Änderungen an Ordnern innerhalb eines Ordners sowie Anzeigen von Besitzer und Berechtigungen	Anzeigen von Eigenschaften, Besitzer und Berechtigungen einer Datei. Ausführen einer Datei, falls es sich um eine ausführbare Datei handelt.
Löschen (D)	Löschen eines Ordners	Löschen einer Datei
Berechtigungen ändern (P)	Ändern der Berechtigungen eines Ordners	Ändern der Berechtigungen einer Datei
Besitz übernehmen (O)	Übernehmen des Besitzes eines Ordners	Übernehmen des Besitzes an einer Datei

Bei markiertem Objekt werden unter Eigenschaften ➡ Sicherheit ➡ Berechtigungen die für das abgefragte Objekt geltenden Zugriffsrechte angezeigt:

Recht	***Verzeichnisrechte***	***Dateirechte***
Kein Zugriff	––	––
Lesen	RX	RX
Ändern	RWXD	RWXD
Vollzugriff	Alle	Alle
Anzeigen	RX	nicht angegeben
Hinzufügen	WX	nicht angegeben
Hinzufügen und Lesen	RWX	RX

Die zweifache Anzeige bei der Verzeichnisberechtigung bezieht sich auf das Verzeichnis und danach auf die zukünftig hinzukommenden Dateien. Zugriffsrechte sollten wegen der Übersichtlichkeit stets an Gruppen vergeben werden, obwohl sich dies nicht immer durchhalten läßt. Grundsätzlich gilt, daß für den Zugriff das entsprechende Recht zugewiesen sein muß, d. h. hat weder Benutzer B noch eine seiner Gruppen D und E ein Zugriffsrecht und hat auch JEDER keine Rechte, bleibt B die entsprechende Datei bzw. das Verzeichnis verschlossen. Sofern ein Benutzer in mehreren Gruppen Mitglied ist, werden bei einer Kollision von Zugriffsrechten immer beide Rechte kumuliert. Ausnahme ist das Recht »Kein Zugriff«, das als Veto alle anderen Rechte übergeht!

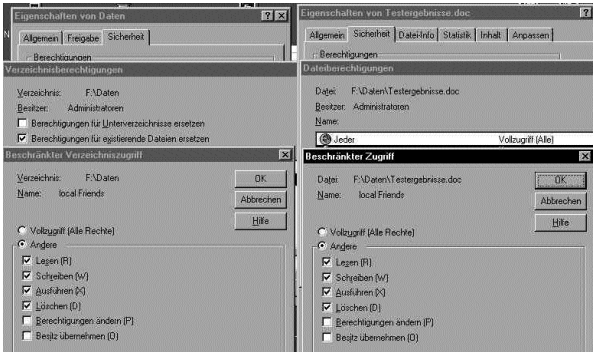


Abbildung 30: Verzeichnis- und Dateizugriffsrechte unter NTFS

Die Möglichkeiten, mal schnell die Besitz- und Zugriffsverhältnisse einzusehen, sind mit den Bordmitteln von Windows NT sehr dürftig und umständlich. Drittanbieter, wie z. B. der Sicherheitsmanager in Abschnitt 7.4 oder DumpACL in Abschnitt 7.2, vereinfachen dies erheblich.

Ähnlich wie bei Dateien und Verzeichnissen lassen sich auch auf andere Ressourcen in NT-Systemen Zugriffsrechte vergeben. Dazu zählt die Registry und auch der Drucker.

2.8 REGISTRY

Die Registry oder Registrierdatenbank ist der Ort, an dem alle Konfigurationsdaten eines NT-Systems abgelegt sind. Dementsprechend sensibel ist jeder Zugriff bzw. jede Änderung. Die Registry ist mit den üblichen Editoren nicht lesbar. Deshalb werden standardmäßig zwei Programme mitgeliefert, die sich in der Regel im Verzeichnis \WINNT\System32 befinden: regedt32.exe und regedit.exe. regedit.exe ist eigentlich der Editor für die Windows95-Registry. Er hat aber eine Such-

funktion, die merkwürdigerweise im NT-eigenen Editor nicht vorhanden ist. Die Registrierdatenbank (Registry) stellt den Ersatz für die INI-Dateien aus den vorhergehenden Windows-Versionen dar. Um die Verwaltung der zahlreichen Einstellungen zu vereinfachen, faßt die Registry alle Einstellungen unter einem Dach zusammen. Unter dem Dach sind die Etagen, Treppen und Zimmer aber zahlreich, verwinkelt, mit zahlreichen Türen und Falltreppen versehen und deshalb nur mit Mühe zu merken. Die Tips und Tricks zur Optimierung von Windows durch Änderung der Registry finden sich in speziellen Büchern, in jedem (Windows-orientierten) Computerheft und auf zahlreichen Homepages im Internet. Der interessierte Leser wird dorthin verwiesen, da sonst der gesetzte Rahmen gesprengt wird.

In Abbildung 31 ist die grobe Struktur der Registry, bestehend aus 5 Hauptschlüsseln, erkennbar:

HKEY_LOCAL_MACHINE enthält wesentliche Hardwareangaben.

HKEY_CLASSES_ROOT enthält die Angaben für die Dateiverknüpfungen, z. B. Dateien, die auf »doc« enden, werden aufgrund dieser Festlegung von Winword 7 geöffnet.

HKEY_CURRENT_USER enthält alle Angaben des aktuell angemeldeten Besitzers.

HKEY_USERS enthält alle Angaben zu allen registrierten Benutzern.

HKEY_CURRENT_CONFIG beinhaltet die für den Start notwendigen Hardware-Profile wie Gerätetreiber.

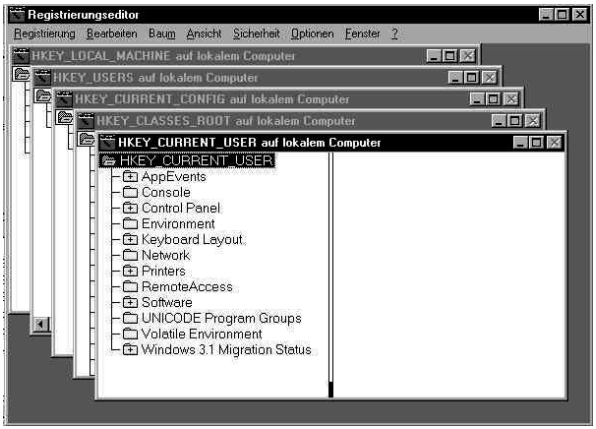


Abbildung 31: Registry geöffnet mit Regedt32

Die Registry wird in den Dateien Sam, security, system und software gespeichert, die standardmäßig im Verzeichnis WINNT\system32\config zu finden sind. Die Dateien mit der Endung »log« sind die entsprechenden Sicherungsdateien, die Dateien mit der Endung EVT sind die Dateien des Ereignisprotokolls.

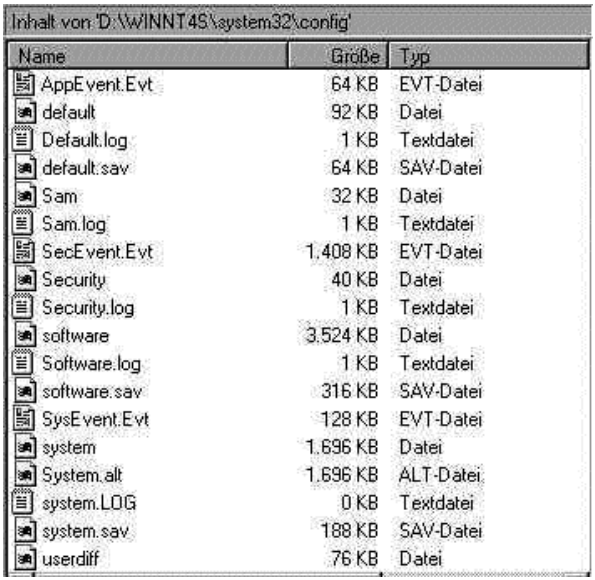


Abbildung 32: Verzeichnis: WINNT\system32\config

Nur die Dateien Ntuser.dat bzw. NTUSER.dat.log, in der die Benutzerdaten der lokalen Benutzer abgelegt sind, werden im Verzeichnis WINNT\Profile\%Benutzername% abgespeichert.

Eine intensive Beschäftigung mit der Registry und ihren Einträgen halten wir für nicht notwendig, da dies in der Regel vom eigentlichen Thema weit ablenkt und viele für die Interessenvertretung wichtige Informationen an anderen Stellen schneller zu finden sind.

Falls dennoch Bedarf an weiteren Informationen zu den aktuellen Einstellungen besteht, gibt es mehrere Wege, an diese Informationen zu kommen. Zum einen lassen sich die einzelnen Bäume der Registry in Dateien oder direkt drucken. Die Einrichtung eines Leserechts auf die Dateien ermöglicht der Interessenvertretung, sich selbst schlau zu machen, ohne aus Versehen Schaden anrichten zu können. Letztlich besteht die Möglichkeit, sich mit der Hilfedatei regedt32.hlp einen Überblick über die Registry zu verschaffen.

2.9 RAS (REMOTE ACCESS SERVICE)

Die Bereitstellung des RAS-Dienstes und die notwendige Aktivierung des RAS-Servers sollte von der Interessenvertretung von Bedeutung sein. Berechtigte Benutzer dürfen von außerhalb auf die Domäne oder den NT-Rechner zugreifen. Sofern sie für die Zugriffsberechtigung und den internen Gebrauch dasselbe Benutzerkonto verwenden und damit dieselben Rechte wie am Arbeitsplatz haben, werden bei einem Zugriff von außerhalb unter Umständen (vereinbarte) Sicherungsmechanismen ausgehebelt.

Der Umfang der RAS-Berechtigung für den einzelnen Benutzer wird unter dem Menü RAS in der Benutzerverwaltung festgelegt. Der RAS-Server als eines der NT-Verwaltungsprogramme überwacht die Aktivitäten beim Fernzugriff. In größeren Firmen wird dafür oft ein gesonderter Rechner installiert, auf dem nur (oder im wesentlichen) das RAS-Server-Programm läuft.

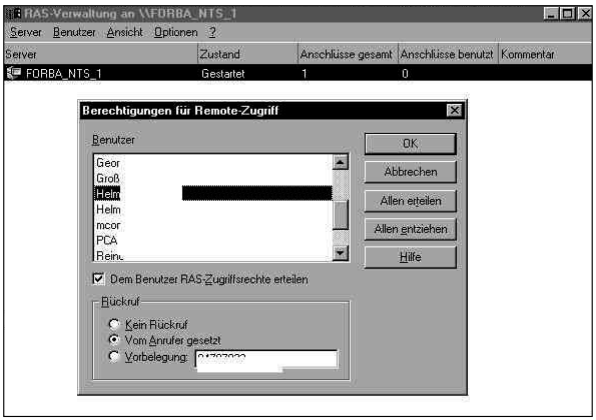


Abbildung 33: RAS-Verwaltung auf dem RAS-Server

Zur Information über die RAS-Berechtigten ist hier ein weitaus schnellerer Zugriff als über die Benutzerverwaltung möglich, obwohl auch hier die gesamte Liste der Benutzer einzeln durchgegangen werden muß. Benutzer mit dem Recht »vom Anrufer gesetzt« können sich von jedem Ort der Welt in das Firmennetz einwählen. Eine Prüfung, die über den Benutzernamen und das Paßwort hinausgeht, findet nicht statt. Demgegenüber kann bei vorgegebener Rückwahlnummer zumindest eine minimale Sicherheit angenommen werden, sieht man von der Möglichkeit der Rufumleitung bei ISDN-Anschlüssen ab.

Benutzer mit der Berechtigung, personenbezogene Daten zu verarbeiten, sollten keinen RAS-Zugriff bekommen.

Falls dies dennoch unumgänglich sein sollte, ist dringend anzuraten, daß der Benutzer für diesen Zugriff ein neues Benutzerkonto bekommt. So kann bei der Rechtevergabe an dieses RAS-Konto geprüft werden, ob bestimmte Laufwerke, Verzeichnisse oder Dateien für den RAS-Zugriff offen sein sollen. Es lassen sich für diese Konten gezielt Überwachungseinstellungen aktivieren, die z. B. für den Alltagsbetrieb nicht aktiviert sind.

Weitere Informationen über RAS sind auch im Verzeichnis WINNT\System32 in den Hilfedateien Rasadmin.hlp (Serververwaltung), Rasphone.hlp (DFÜ-Netzwerk) und Ras-Rasgloss.hlp (Glossar) zu finden.

Als Informationsquelle zur grundsätzlichen Funktionalität sind die zahlreichen Hilfedateien geeignet. Sie lassen sich auf jedem Windows-Rechner öffnen, unabhängig davon, ob das dazugehörende Programm vorhanden oder installiert ist. Die Interessenvertretung sollte sich, sofern sie über eigene PCs verfügt, vom Arbeitgeber im Rahmen der Erstinformation die entsprechenden Dateien geben lassen.

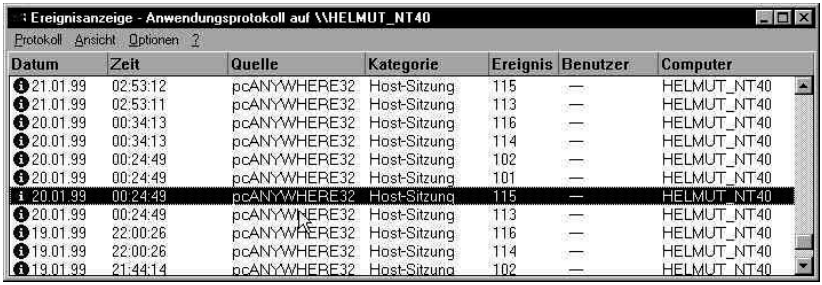
Wird mittels RAS auf die Domäne zugegriffen, finden sich im Systemprotokoll des PDC bzw. BDC z. B. folgende Ereignisse (diese Liste ist nicht vollständig!), die Anlaß zu weiteren Nachforschungen geben können:

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
20097	Benutzer konnte sich in der RAS-Verbindung nicht authentisieren
20098	Benutzer konnte sich in der RAS-Verbindung nicht authentisieren

Gleichzeitig mit den Einträgen im Systemprotokoll sollte auch das Anwendungsprotokoll eingesehen werden. Eine RAS-Verbindung erfolgt z. B. mit Programmen wie PCAnywhere oder CarbonCopy. Diese Programme hinterlassen im Anwendungsprotokoll ihre Spuren mit eigenen Ereignismeldungen/-nummern.

Die anwendungsspezifischen Ereignisnummern von Drittprogrammen wie z. B. PCAnywhere und CarbonCopy werden in den Online-Hilfen von Windows NT nicht geführt. Dazu geben die Hilfe-Dateien der entsprechenden Programme Auskunft.

Aktionen von Fremdprogrammen sind im Anwendungsprotokoll in der Regel unter ihrem Namen eingetragen.



Datum	Zeit	Quelle	Kategorie	Ereignis	Benutzer	Computer
21.01.99	02:53:12	pcANYWHERE32	Host-Sitzung	115	—	HELMUT_NT40
21.01.99	02:53:11	pcANYWHERE32	Host-Sitzung	113	—	HELMUT_NT40
20.01.99	00:34:13	pcANYWHERE32	Host-Sitzung	116	—	HELMUT_NT40
20.01.99	00:34:13	pcANYWHERE32	Host-Sitzung	114	—	HELMUT_NT40
20.01.99	00:24:49	pcANYWHERE32	Host-Sitzung	102	—	HELMUT_NT40
20.01.99	00:24:49	pcANYWHERE32	Host-Sitzung	101	—	HELMUT_NT40
20.01.99	00:24:49	pcANYWHERE32	Host-Sitzung	115	—	HELMUT_NT40
20.01.99	00:24:49	pcANYWHERE32	Host-Sitzung	113	—	HELMUT_NT40
19.01.99	22:00:26	pcANYWHERE32	Host-Sitzung	116	—	HELMUT_NT40
19.01.99	22:00:26	pcANYWHERE32	Host-Sitzung	114	—	HELMUT_NT40
19.01.99	21:44:14	pcANYWHERE32	Host-Sitzung	102	—	HELMUT_NT40

Abbildung 33a:
Protokollierung des RAS-Zugriffs mit PCAnywhere

3 SICHERHEIT – EINRICHTEN UND ÜBERWACHEN

Betrachtet man die (unvollständige) Auflistung von Sicherheitsmerkmalen, die bei Windows NT zur Verfügung stehen, so ergeben sich, trotz aller berechtigter Kritik an Windows NT, vielfältige Möglichkeiten, eine Datenverarbeitung sicher zu gestalten. Zumindest im Alltag eines Unternehmens kann ein Mindeststandard an Sicherheit und Datenschutz gewährleistet werden, wenn die von NT angebotenen technischen Möglichkeiten denn angewendet werden.

3.1 SICHERHEITSMERKMALE VON WINDOWS NT (UNVOLLSTÄNDIGE AUFLISTUNG)

Benutzerkennung	ja
Paßwort mit Längenvorgabe <n>	ja
Einmalpaßwort für neuen Benutzer	ja
Sperre nach <n> Fehlversuchen bei Login	ja
Paßwortwechsel jederzeit vom Benutzer durchführbar	bedingt
Periodischer Paßwortwechsel / max. Paßwortalter	ja
Kennwortchronik	ja
Differenzierte Paßwortgestaltung	nein
Prüfung Trivialpaßwörter / Wörterbücher	nein
Benutzerspezifisches Monitoring	nein
Möglichkeit der Einschränkung der Konten DomänenAdmin und Admin	nein
Revisions/Auditor-Konto	nein
Benutzerspezifische Liste der erteilten Zugriffsberechtigungen / Freigaben	nein
Zeitliche Begrenzung des Zugriffs	ja
Differenzierte Zugriffsrechte auf Verzeichnisebene	ja
Differenzierte Zugriffsrechte auf Dateiebene	ja
Differenzierte Zugriffsrechte auf Drucker	ja
Differenzierte Zugriffsrechte bis auf die unterste Ebene der Registry	ja
Differenzierte Protokollierung der Zugriffe	ja
Individuelle Oberflächengestaltung	ja
Individuelle Sperrung von Laufwerken	bedingt

Individuelle Sperrung von Schnittstellen	bedingt
Unterbinden der Rechnerabschaltung ohne Anmeldung	ja
Speicheraufbereitung bei Benutzerwechsel	ja
Bildschirmsperre	ja
Arbeitszeitbeschränkung (nur bei Anmeldung auf einem Domänenkonto)	ja
Datensicherungsfunktionen	ja
Virenschutz	nein

3.2 C2-ZERTIFIZIERUNG

Das Argument, Windows NT sei C2-zertifiziert und damit sicher, wird oft gegenüber Interessenvertretungen vorgebracht, um Forderungen an den Datenschutz und die Nachvollziehbarkeit der Datenverarbeitung abzuwehren. C2 wirkt dabei oft als »Totschlagargument«, denn was sollte eine Interessenvertretung dagegen sagen. Wie so oft soll die Interessenvertretung sich nicht abspeisen lassen, sondern sachkundig machen. Hebt man den C2-Vorhang hoch, so sieht es dahinter schon nicht mehr so eindrucksvoll aus.

Windows NT Workstation 3.51 ist in den USA nach C2 zertifiziert worden. Heute wird meist NT 4 und dann der Server eingesetzt. C2 ist eine niedrige Sicherheitsstufe des sogenannten Orange Books des US-Verteidigungsministeriums. Im Orange Book wurden sieben Sicherheitsstufen für Computersysteme festgelegt: D (geringste Sicherheit), C1, C2, B1, B2, B3 und A1 (höchste Sicherheit). Für die Zertifizierung nach C2 muß ein Produkt folgende Bedingungen erfüllen:

- Jeder Benutzer muß sich vor der Benutzung eines Rechners mit seiner Benutzerkennung und seinem Paßwort identifizieren und authentisieren.
- Es muß eine detaillierte Rechteverwaltung auf Datei- und Verzeichnisebene für einzelne Benutzer bzw. Benutzergruppen möglich sein. Die Rechteverwaltung muß derart gestaltet sein, daß der Zugriff gänzlich verweigert werden kann.
- Die Rechte- und die Benutzerverwaltung dürfen nur durch autorisierte Benutzer erfolgen.
- Bei jedem Zugriff muß die Berechtigung überprüft werden. Unberechtigte Zugriffe müssen abgewiesen werden.
- Alle Aktionen innerhalb einer Sitzung, auch die von autorisierten Benutzern, müssen protokolliert werden können. Die Protokolle dürfen nur autorisierten Benutzern zugänglich sein. Die Programme zur Auswertung der Protokolle müssen vorhanden

und dokumentiert sein. Es muß möglich sein, einzelne Aktionen einzelner Benutzer oder Gruppen zu filtern.

- Vor der Benutzung durch einen anderen Benutzer muß der Speicherinhalt so aufbereitet werden, daß keine Rückschlüsse auf den früheren Inhalt möglich sind.

Windows NT 3.51 erfüllt diese Bedingungen und ist in den USA für C2 zertifiziert, allerdings nur für eine alleinstehende Workstation, die auch vollständig unter NTFS läuft. Vernetzte NT-Rechner in einer Domäne oder in einem Peer-to-Peer-Netzwerk sind nicht C2-zertifiziert.

Auf der CD »Technische Referenz« ist ein kleines Prüfprogramm C2 enthalten, das zum einen die aktuellen Sicherheits-Einstellungen abfragt, zum anderen die direkte Änderung dieser Einstellungen in der Registry ermöglicht. Als Minitest für die Anzeige der C2-Sicherheit eines NT-Rechners ist C2.EXE unseres Erachtens geeignet. Änderungen an der Registry sollten damit allerdings nicht vorgenommen werden, da es mit diesem englischen Programm auf deutschen NT-Systemen zu Problemen kam.

3.3 SYSTEMRICHTLINIEN

In vielen Betrieben besteht von der Arbeitgeberseite her das Problem, daß Benutzer mit den standardmäßig eingerichteten NT-Workstations auch Zugang zu den Verwaltungsprogrammen von Windows NT Workstation bekommen oder sich verschaffen. Veränderungen der Benutzer an der Schreibtischoberfläche (dem Desktop) oder Hinzufügung von Bildschirmschonern, die zu Systemabstürzen oder Rechnerproblemen führen, bereiten PC-Betreuern Probleme. Um dieser Situation entgegenzuwirken, die Kosten für die Rechnerbetreuung zu senken (TCO = Total Cost of Ownership) und die Installation von einheitlichen Umgebungen zu ermöglichen, liefert Microsoft auf der Server-CD das Programm Poledit. Poledit ist ein mächtiges Werkzeug, um zentrale Vorgaben (Richtlinien) für Client-Rechner (nur Windows 95 und NT Workstation) und Benutzer zu erstellen.

Nicht behandelt wird hier ZAK (Zero Administration Kit), ein mächtiges und dazu kostenloses Werkzeug von Microsoft, mit dem Systemrichtlinien, Benutzerprofile und Sicherheitsmaßnahmen zentral angelegt, verwaltet und gepflegt werden können.

Poledit macht eigentlich das gleiche wie die beiden oben vorgestellten Registry-Editoren Regedt32 und Regedit, es verändert die Registry. Der Unterschied besteht darin,

daß mit Poledit Benutzer-, Gruppen- und Computer-Systemrichtlinien für unterschiedliche Benutzer/Gruppen und Computer erstellt werden, die dann beim Startvorgang jedesmal benutzer-, gruppen- und/oder computerspezifisch geöffnet werden und die Registry – für die aktuelle Sitzung – entsprechend einstellt (verändert). Meldet sich anschließend ein anderer Benutzer an, werden die Einstellungen der Registry wieder entsprechend der Systemrichtlinie für diesen Benutzer, seine Gruppe oder den Rechner verändert.

Damit die Richtlinien für NT-Rechner und Benutzer in der gesamten Domäne in Kraft treten, müssen sie als Datei NTCONFIG.POL im PDC-Verzeichnis NETLOGON (= \WINNT\System32 \repl\inport\scripts) abgelegt werden.

Sofern zusätzlich auch Windows95-Rechner durch Richtlinien gesteuert werden sollen, muß eine Datei CONFIG.POL in NETLOGON gespeichert werden. Die Speicherung in NETLOGON nutzt den Fakt, daß NT bei jeder Anmeldung nach Login-Skripten oder Richtliniendateien auch den Namen der Benutzer, Gruppen oder Rechner in NETLOGON sucht. Findet NT entsprechende Dateien, dann überlagern deren Vorgaben das lokal angelegte Benutzerprofil NTUSER.DAT des Benutzers.

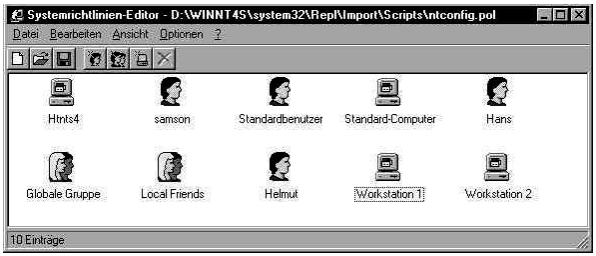


Abbildung 34: Gruppen, Benutzer und Rechnerrichtlinien

Die Benutzer- bzw. Gruppenrichtlinien gelten überall in einer Domäne, egal an welchem Rechner sich ein Benutzer oder ein Gruppenmitglied anmeldet. Computer-Richtlinien beziehen sich auf einen konkreten Rechner. Benutzer-/Gruppen- und Computerrichtlinien können gleichzeitig angewendet werden, da beliebig viele Benutzer, Gruppen und Computer in einer gemeinsamen Richtliniendatei gespeichert werden können.

Die Einstellmöglichkeiten bei »Benutzer« und »Computer« zeigen auch die dahinterliegenden Registry-Schlüssel HKEY_LOCAL_MACHINE und HLKEY_CURRENT_USER

In den Systemrichtlinien für »Computer« gibt es die Möglichkeit, einen speziellen Pfad zu definieren, um ein Update der Registry mit Hilfe des Systemrichtlinien-Editors

regelmäßig automatisch durchführen zu können. Dieser Schalter ist interessant, wenn mehrere Windows NT-Rechner von einer Quelle im Netzwerk gepflegt werden sollen. Man erreicht so ein konsistentes Rechtekonzept, sofern alle Rechner mit den gleichen Rechten ausgestattet sind.

Microsoft liefert drei Standardprofile, die als Muster für eigene Richtlinien herangezogen werden können. Die Dateien WINT.ADM, WINDOWS.ADM und COMMON.ADM sind reine Textdateien und lassen sich mit jeder Textverarbeitung/jedem Editor öffnen. Prinzipiell lassen sich so durch Erstellung eigener Vorgabedateien, die dann in den Richtlinieneditor Poledit geladen werden, alle Eintragungen in der Registry beeinflussen.

Abbildung 35:
Einstellmöglichkeiten für Computer

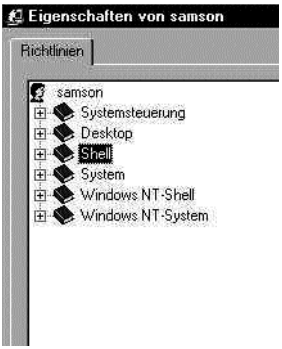


Abbildung 36:
Einstellmöglichkeiten für Benutzer

Im Extrem lassen sich Systemrichtlinien für eine NT Workstation erstellen, die einem Benutzer keine Oberfläche und keine Wahlmöglichkeit nach der Anmeldung geben, sondern gleich ein bestimmtes Programm aufrufen. Ergänzt durch restriktive NTFS-Zugriffsberechtigungen bzw. Einschränkungen hat der Benutzer bei dieser Einstellung nur auf ein einziges Verzeichnis Zugriff, um nur dort Dateien zu verarbeiten.

Wenn es um die Frage der Abschottung von Rechnern oder der Einschränkung von Benutzern während der Arbeit mit sensiblen Daten geht, sollte die Anwendung von Poledit zur Erzeugung entsprechender Richtlinien als Lösungsweg geprüft werden.

Da es sich bei den Systemrichtlinien um reine Textdateien handelt, lassen sich für firmenspezifische Systemrichtlinien vollkommen neue Musterdateien (*ADM) erstellen.

Die Muster sind standardmäßig unter WINNT\INF gespeichert. In den Textdateien lassen sich beliebige Einstellungen in jeder Tiefe der Registry über die Benutzeranmeldung steuern.

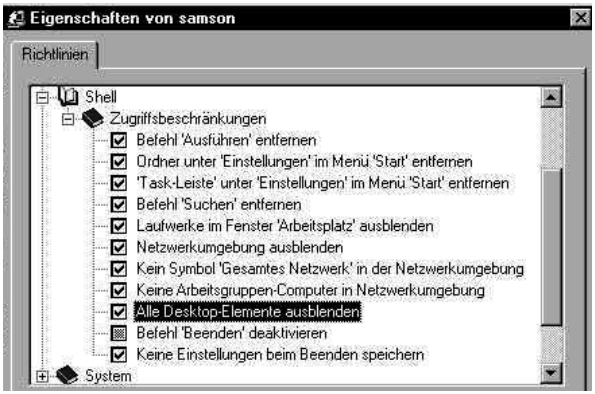


Abbildung 37: Bearbeitungsmaske des Benutzerprofils

3.4 BENUTZERPROFILE

Bei der Begehung eines NT-Systems taucht – wie auch in anderen Situationen, wenn man vor einem Bildschirm steht und ein fingerfertiger Kollege einen durch die Menüs, Fenster und Anwendungen »führt« – die Frage auf, als welcher Benutzer wir gerade im System sind. Die Frage ist schon deshalb wichtig, da, wie oben bei den Benutzergruppen erläutert, nicht jede Gruppe gleiche Rechte hat und dementsprechend auch mit unterschiedlichen Sichten auf das NT-System ausgestattet ist. Bei einer Begehung dürfen keine Beschränkungen der Sicht und des Zugriffs bestehen.

Wird bei gedrückter rechter Maustaste auf die START-Taste geklickt und danach auf EXPLORER, springt das Programm in das Verzeichnis WINNT\System32 \Profiles\ <aktueller Benutzer>, hier »Helmut«. Welcher Gruppe »Helmut« angehört, ist aus dem Benutzermanager zu erfahren, der entweder unter START ➡ AUSFÜHREN ➡ Eingabe: »usrmngr« oder über START ➡ Programme ➡ Verwaltung (allgemein) ➡ Benutzermanager für Domänen aufgerufen wird. Im Benutzerprofil des vorher angezeigten Benutzers findet sich unter »Gruppe« die gewünschte Information zur Gruppenzugehörigkeit und Kompetenz des aktuellen Benutzerkontos. Ist kein Zugang zum Benutzermanager möglich, besteht entweder kein Zugang zu einem Server oder der Kollege, der die Tastatur bedient, hat keine Administrationskompetenz. In einem solchen Fall

müßte die Begehung abgebrochen und ein Kollege oder eine Kollegin mit uneingeschränkten Rechten dazugeholt werden.

Im rechten Fenster stehen i. d. R. als einzige Dateien »ntuser.dat« und »ntuser.dat.LOG«. Es handelt sich hier um das Benutzerprofil des angemeldeten Benutzers. Dieses Profil beinhaltet die gesamte individuelle Benutzerumgebung, u. a. alle Benutzereinstellungen, die im Explorer gewählt wurden, alle Programmgruppen und Einträge, alle Verbindungen zu Netzdruckern, alle benutzerspezifischen Einstellungen des Schreibtischs, des Cursors, des Bildschirmschoners und vieles mehr.

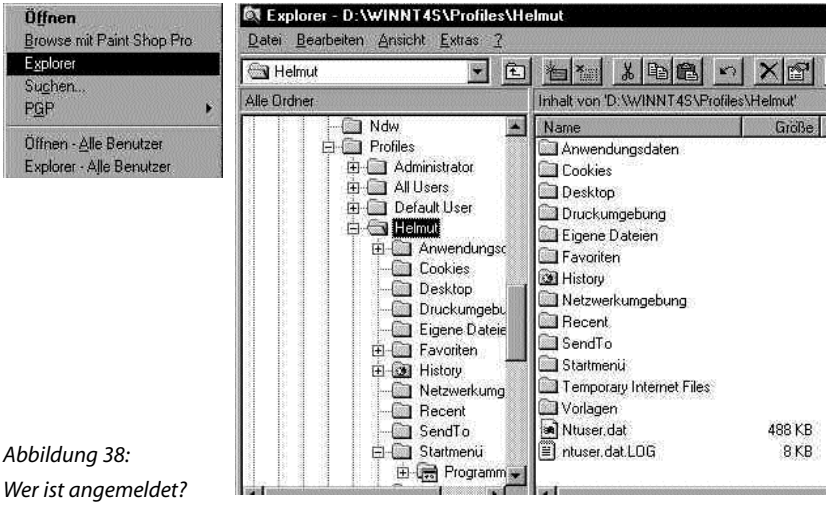


Abbildung 38:
Wer ist angemeldet?

Im Verzeichnis »Profiles« stehen über oder unter dem aktuellen Benutzer auch andere Benutzernamen. Diese Verzeichnisse enthalten die Benutzerumgebungen aller an diesem Rechner irgendwann mal angemeldeten Benutzer. In diesem Zusammenhang läßt sich ein kurzer Blick ins Thema »Kontrollmöglichkeit gegenüber Benutzern« werfen, indem man einen Blick in Unterverzeichnisse wie Favoriten, Recent, Temporary Internet Files oder Cookies wirft. Dort steht mit Datum und Uhrzeit, wo der betreffende Benutzer im Internet gesurft hat oder welches seine favorisierten Homepages sind. Das Verzeichnis »Profiles« kann durch den Arbeitgeber jederzeit eingesehen werden. Der Benutzer bemerkt dies nicht!

Benutzerprofile können lokal oder serverbasierend definiert werden. Um was für ein Profil es sich bei dem gerade im Explorer unter Profiles angesehenen handelt, ist z. B. aus dem Bild »Benutzerprofile« in EIGENSCHAFTEN ➡ ARBEITSPLATZ zu ersehen.

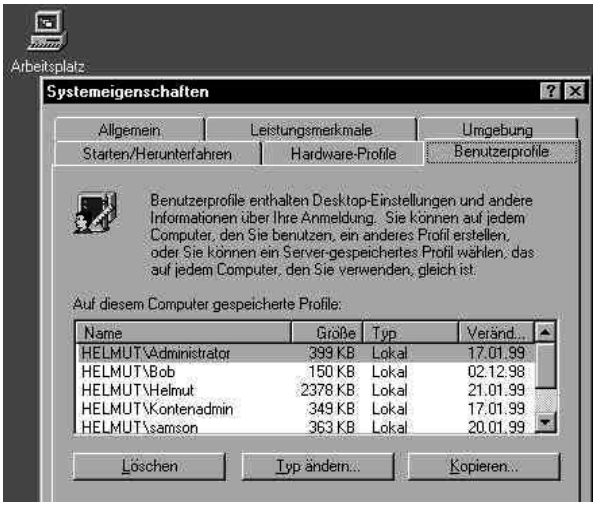


Abbildung 39: Benutzerprofile und -arten abfragen

Hier sieht man auch, wann ein Profil zuletzt verändert wurde. An dieser Stelle lassen sich Profile von lokalen zu serverbasierenden Profilen ändern, löschen und an andere Stellen kopieren, z. B. auf andere Pfade des Servers oder des lokalen Rechners.

Die Einrichtung von lokalen Benutzern auf einem PDC oder BDC sollte auf den Administrator und den (deaktivierten) Gast beschränkt bleiben, da für andere als die Administratoren keine Notwendigkeit besteht, direkt am Server zu arbeiten.

Serverbasierende Profile werden auf dem PDC der Domäne in dem Verzeichnis gespeichert, das im Benutzermanager als »Pfad für Benutzerprofil« angegeben ist. Ohne eine Pfadangabe an dieser Stelle bleibt ein Profil lokal. Serverbasierende Profile werden in NT-Diktion auch als »roaming profiles« bezeichnet, denn durch die Speicherung auf dem PDC kann sich der Benutzer grundsätzlich – soweit ihn nicht sein Benutzerkonto in den Einstellungen zu »Anmelden an« einschränkt – an jedem Rechner in der Domäne anmelden. Dabei erhält er, egal an welchem Rechner er sich anmeldet, seine individuelle Benutzerumgebung. Bei der Anmeldung wird eine Kopie seines Profils auf den jeweiligen lokalen Rechner kopiert. Diese Art der serverbasierenden Profile wird auch persönliche Profile genannt. Würde einmal keine Verbindung zum PDC oder einem BDC möglich sein, könnte der Benutzer sich zumindest lokal am Rechner anmelden und arbeiten, da der lokale Rechner die letzten zehn Anmeldungen als Profile speichert. Die dem Benutzer zugewiesenen Ressourcen in der Domäne stünden in einem solchen Fall natürlich nicht zur Verfügung.

Um den Benutzern die Vorteile der domänenweiten Anmeldung bei gleichzeitigem Ausschluß der Einflußnahme auf ihre Benutzerumgebung zu ermöglichen, werden Benutzerprofile auch als »obligatorische Profile« (mandatory profil) angelegt. Dazu wird ein Benutzerpfad im Benutzermanager unter PROFIL eingetragen. Aus NTUSR.DAT wird NTUSR.MAN mit der Konsequenz für den Benutzer, daß er keinerlei Veränderungen an seiner Benutzerumgebung (z. B. keinen anderen Hintergrund, keinen Bildschirmschoner, keinen anderen Drucker, keine neuen Netzlaufwerke usw.) vornehmen kann.

3.5 ÜBERWACHUNG UND KONTROLLE

Die Verarbeitung von personenbezogenen Daten außerhalb der abgeschotteten Großrechner und Midrange-Computer wie z. B. einer IBM AS/400 ist längst überall Praxis. Für die Interessenvertretung ergab sich dadurch die Situation, daß nicht mehr ein oder wenige Rechner beobachtet und geregelt werden konnten. Statt dessen machten unzählige PCs eine wirksame Überprüfung eingehaltener Vereinbarungen nahezu unmöglich. Vor allem eine wirksame Überwachung ist auf Windows PCs standardmäßig nicht gegeben.

Windows NT bietet von Hause aus die Möglichkeit, den einzelnen Windows NT-Rechner in verschiedensten Situationen zu überwachen. Werkzeuge der Überwachung sind die Einstellungen in der Registry, die Ereignisprotokolle und die Ereignisanzeige (EventViewer).

Einer der Negativpunkte von Windows NT ist die fehlende Revisions-Autorität eines standardmäßig konfigurierten Revisors oder eines Auditors, der standardmäßig für die Überwachung der Administratoren und die Überwachungsprotokolle zuständig ist.

Die Korrektur dieses Mankos durch Löschung der Konten der Administratoren und Festlegung neuer Administratoren ist unmöglich, da diese Gruppen- und Einzelkonten als Systemgruppen (ebenso wie die Gastkonten, die Benutzerkonten und die Subadministratorenkonten) nicht löschbar sind.

Es bleiben aus unserer Sicht zwei Problem-Lösungen: 1. Es muß den Menschen, die zur Gruppe Administratoren bzw. Domänen-Administratoren gehören, vollstes Vertrauen entgegengebracht werden. Dies ist nicht immer eine befriedigende Lösung, manchmal aber nicht zu verhindern

Die unseres Erachtens bessere, aber auch aufwendigere Lösung weist anderen Gruppen die ursprünglichen Administrator-Rechte zu. Auf jedem NT-Rechner in der Domäne wird anschließend das Konto Administrator bzw. auf dem PDC das des Domänen-Administrators gesperrt.

Sperren heißt, daß die existierenden Sub-Administratoren – soweit noch nicht geschehen – mit allen für die jeweilige Administrationsaufgabe notwendigen Berechtigungen, Freigaben und Zugriffsrechten auf Ressourcen ausgestattet werden. Gleiches erfolgt für die Gruppe Domänen-Revisoren und Lokale Revisoren.

Danach wird das Administratorpaßwort bzw. das des Domänen-Administrators wie folgt geändert: Mehrere Personen – in vielen Sicherheitsartikeln wird die Zahl drei genannt – geben im Benutzermanager jeweils ein Teilpaßwort ein, das den anderen beiden Personen nicht mitgeteilt wird. Die drei Paßwortteile werden in einem versiegelten Umschlag bei der Geschäftsleitung für Notfälle in den Tresor gelegt.

Mit diesem Verfahren wird die Funktionsfähigkeit eines NT-Systems nicht eingeschränkt, denn die Sub-Administratoren haben die Möglichkeit, alle Administrationsaufgaben wahrzunehmen. Allerdings ist für jede Tätigkeit eine neue Anmeldung unter dem jeweiligen Konto notwendig. Diesen Aufwand lehnen die meisten Administratoren ab. Im Rahmen der verschlankten EDV-Abteilungen steht oft nur noch wenig Personal zur Verfügung und wenige erledigen die Aufgaben von vielen, auch in der Administration.

Insbesondere außerhalb von Großbetrieben sind die zuständigen Administratoren an einer Hand abzuzählen, so daß die Interessenvertretung unter Umständen in ein Dilemma gerät. Das Problem ist die höhere Sicherheit im System auf der einen Seite oder ein gutes Verhältnis zu den Kolleginnen und Kollegen aus der EDV auf der anderen Seite. Falls die »Deaktivierung« der Konten der Administratoren nicht gelingt, bleibt die folgende nicht perfekte und deshalb etwas unbefriedigende Lösung:

Auf jedem lokalen Rechner wird eine Gruppe REVISION und auf dem PDC wird eine globale Gruppe REVISION angelegt. Nur die globale Gruppe REVISION wird Mitglied in der lokalen Gruppe REVISION der einzelnen NT-Rechner. Ausschließlich die lokale Gruppe REVISION erhält für den jeweiligen Rechner das Benutzerrecht »Verwalten von Überwachungs- und Sicherheitsprotokoll (BENUTZERMANAGER ➧ RICHTLINIEN ➧ BENUTZERRECHTE)«. Ohne Protokollierung in das Ereignisprotokoll könnte REVISION dieses Recht nicht entzogen werden. Wenn Protokolle regelmäßig von der REVISION archiviert werden, kann nur mit sehr großem Aufwand manipuliert werden. Die archivierten Logs müssen in einem überwachten Verzeichnis abgelegt werden, zu dem nur die REVISION Vollzugriff und die Administratoren Leserecht haben.

3.5.1 Überwachung einstellen

Die Überwachung und damit Erzeugung von Einträgen, sogenannten »Ereignissen« , in das Ereignisprotokoll benötigt als ersten Schritt die Aktivierung der Protokollierung. Diese erfolgt im Benutzermanager unter RICHTLINIEN – ÜBERWACHEN.

Die Überwachung kann sich auf folgende Objekte erstrecken: Verzeichnisse, Dateien, Drucker, die Registry, Richtlinien für Konten, Richtlinien für Benutzerberechtigungen, Benutzer- und Gruppenverwaltung. Nicht überwacht werden können alle Objekte, die auf einem Laufwerk gespeichert sind, das nicht NTFS-formatiert ist. Windows 95/98-Rechner lassen sich nicht überwachen. Macintosh-Rechner und Novell-Laufwerke lassen sich ebenfalls von Windows NT aus nicht überwachen.

Die Überwachung bezieht sich immer nur auf Objekte, die von dem Rechner, auf dem die Überwachung eingerichtet wird, verwaltet werden, d. h. Verzeichnis-, Datei- und Druckerüberwachung muß gegebenenfalls auf jedem einzelnen Rechner eingerichtet werden.

Die Überprüfung, ob ein bestimmtes Objekt überwacht wird, findet im gleichen Dialog wie die Überwachungsaktivierung statt. Nachdem das gewünschte Objekt markiert ist, wählt man entweder aus dem Kontextmenü (wird durch Drücken der rechten Maustaste geöffnet) oder aus dem Menüpunkt DATEI den Eintrag EIGENSCHAFTEN. Hier verbirgt sich hinter dem Karteireiter SICHERHEIT die Schaltfläche ÜBERWACHEN. Wird dieser Punkt angewählt, gelangt man in den Einstellungs-Dialog. Hier sind zuerst die Gruppen oder Benutzer auszuwählen, welche für eine Überwachung in Frage kommen. Danach wird die Art der Überwachung festgelegt.

Abbildung 40: Überwachung einstellen

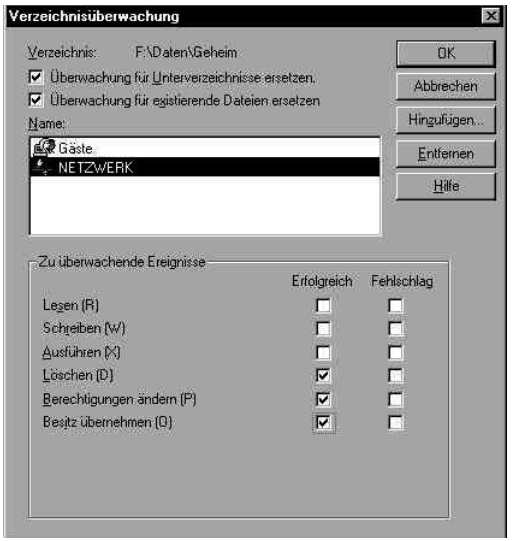


Abbildung 41: Verzeichnisüberwachung

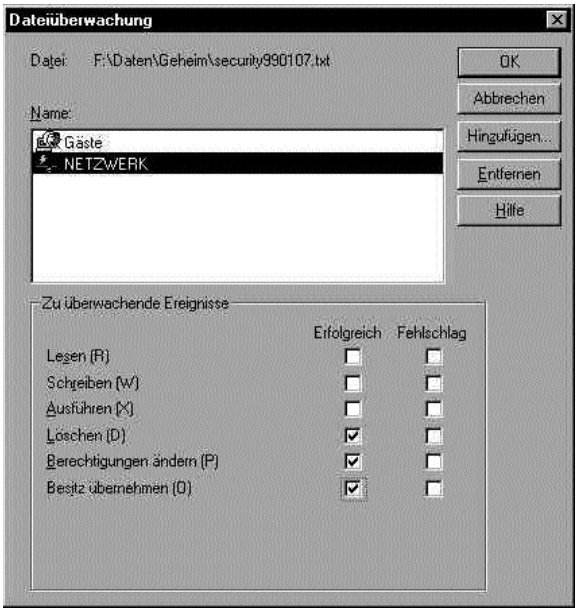


Abbildung 42: Dateiüberwachung

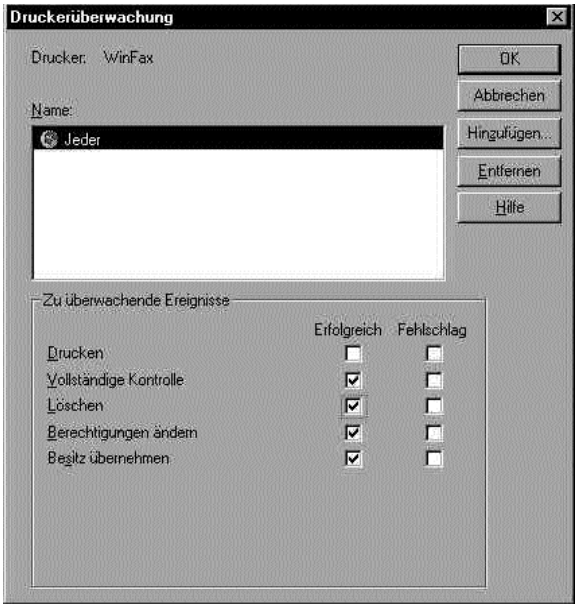


Abbildung 43: Überwachung Drucker und Fax

Die Interessenvertretung hat bei der Festlegung, welche Benutzer oder Gruppen überwacht werden sollen, gemäß BetrVG bzw. PersVG mitzubestimmen.

Die Forderung einer Interessenvertretung nach Überwachung scheint ein Widerspruch zur Forderung »Keine Verhaltens- und Leistungskontrolle« zu sein. Wir meinen, dies ist kein Widerspruch, denn die Interessenvertretung hat die Aufgabe, die Einhaltung unterschriebener Vereinbarungen, aber auch die von gesetzlichen Vorgaben, wie z. B. den Datenschutz, zu überwachen. Wenn ein System diese Möglichkeit anbietet, sollte sie unseres Erachtens auch verantwortungsvoll genutzt werden.

Die Bilder zeigen die unterschiedlichen Details der Überwachung. Die Datei und Druckerüberwachung bezieht sich immer auf das eine Objekt. Verzeichnisüberwachung kann auch untergeordnete Verzeichnisse und/oder die darin enthaltenen Dateien umfassen.

Im Gegensatz zum Windows95-Editor Regedit bietet der NT-Editor REGEDT32.EXE einen Menüpunkt, um die Registrierdatenbank zu überwachen. Die Überwachung der gesetzten Werte ist aber ausgeschlossen, d. h. im Ereignisprotokoll ist zu erkennen, in welchem Schlüssel oder Teilschlüssel Änderungen vorgenommen wurden, aber nicht welche Art.

Alle drei Ereignisprotokolle »Sicherheit«, »System« und »Anwendung« können mit NT-eigenen Werkzeugen archiviert werden. Dazu bedarf es keines Aufwands, außer es zu tun.

Die Archivierung eines Protokolls kann in eine EVT-Datei, die von der Ereignisanzeige gelesen werden kann, in eine CSV-Datei, die z. B. von EXCEL gelesen werden kann, oder eine TXT-Datei geschrieben werden. Einzelne ausgewählte Teile eines Protokolls können nicht archiviert werden, sondern nur das gesamte aktive Protokoll. Die Archivierung einzelner Protokolle ist dagegen möglich. Als EVT-Dateien abgespeichert, können archivierte Protokolle im üblichen Dialog DATEI ÖFFNEN in die Ereignisanzeige wieder eingelesen werden. Daraus läßt sich wie bei aktiven Protokollen eine lesbare Textdatei erzeugen.

In welchem Rhythmus eine Archivierung vorgenommen werden sollte, kann nicht generell empfohlen werden. Dies hängt vom Sicherheitsbedürfnis der beteiligten Parteien ab. Hier ist Ausprobieren notwendig. Die Erfahrung hat aber gezeigt, daß angesichts großer Platten eine Beschränkung auf 512 KB eher der Abwimmlung der Interessenvertretung dient, als einer sinnvollen Nutzung dieses Instruments. Microsoft ermöglicht bis zu 420 MB große Protokolldateien. Ursprünglich sind die Ereignisprotokolle

unter WINNT\system32\config abgespeichert. Dies ist aber nur der standardmäßige Pfad, der sich jederzeit in der Registry ändern läßt.

```
03.12.98        19:27:44        Security    Überwachung-Erfolgreiche Kontenverwaltung
        643     Administrator   HTNTS4      Domänenrichtlinie geändert:
        Domäne: HELMUT
        Domänen-ID: S-1-5-21-306731935-94839519-953900138
        Benutzername des Aufrufers: Administrator
        Domäne des Aufrufers: HELMUT
        Anmelde-ID des Aufrufers: (0x0,0x2406)
        Privilegien: –

03.12.98        19:27:28        Security    Überwachung-Erfolgreiche
                                            Richtlinienänderung
        612     Administrator   HTNTS4      Änderung der Überwachungsrichtlinien:
        Neue Richtlinie:
                Erfolg  Fehlschlag
                +       +       System
                +       +       Anmeldung/Abmeldung
                +       +       Objektzugriff
                +       +       Verwendung eines Privilegs
                –       –       Ausführliche Verfolgung
                +       +       Richtlinienänderung
                +       +       Kontenverwaltung
Geändert von:
        Benutzername: Administrator
        Domänenname: HELMUT
        Anmelde-ID: (0x0,0x2406)
```

Abbildung 44: Export des Sicherheitsprotokolls in eine Text-Datei

Es ist zu empfehlen, daß ein gesondertes Archiv-Verzeichnis erstellt wird. Die REVISOREN werden Besitzer des Verzeichnisses, seiner Unterverzeichnisse und der darin enthaltenen Dateien.

Andere Domänen-Benutzer und auch die Administratoren erhalten nur ein Leserecht. Das Verzeichnis und alle darin enthaltenen Dateien werden überwacht.

3.5.2 Überwachung prüfen mit der Ereignisanzeige

In der Ereignisanzeige werden alle Aktionen des Systems protokolliert, soweit dafür eine sogenannte ID Nummer vorliegt. Dabei unterteilt sich die Ereignisanzeige in drei Bereiche: System, Sicherheit und Anwendung. Es wird zu jedem protokollierten Ereignis ein Zeitstempel, eine Quelle und der Rechner, auf den die Aktion ausgelöst wurde, verzeichnet. Die einzelnen Ereignisse sind über einen Katalog von Meldungen verschlüsselt. Eine Liste aller möglichen Meldungen ist im Microsoft Windows NT Resource Kit 4.0 unter *Online Docs* in der Hilfedatei *Windows NT Messages* aufgezeigt.

3.5.3 Dateien der Ereignisanzeige

Die Ereignisprotokolle werden in drei separaten Dateien gespeichert.

SysEvent.Evt	System-Log-Datei
SecEvent.Evt	Sicherheits-Log-Datei
AppEvent.Evt	Anwendungs-Log-Datei.

Normalerweise werden die Dateien unter *WINNT\system32\config* gespeichert. Auf diese Dateien haben Domänenbenutzer standardmäßig keinen Zugriff. Die Log-Dateien für die System- und die Anwendungsereignisse können von der Gruppe der Administratoren und Operatoren gelesen werden. Dem Systemadministrator ist das Lesen der Log-Datei für die Sicherheit vorbehalten.

3.5.4 Zeichen der Ereignisanzeige

Für einen schnellen Überblick über wichtige Ereignisse sind die Meldungen mit Symbolen gekennzeichnet.

Fehler	Bedeutendes Problem bei der Bearbeitung von Daten oder bei der Ausführung einer Funktion (z. B. Dienst konnte nicht gestartet werden)
Warnung	Problem ist nicht schwerwiegend, kann jedoch in der Zukunft zu Problemen führen (z. B. Plattenplatz nur noch gering)

	Information	Zeigt das erfolgreiche Laden eines Dienstes oder Services (z. B. Laden einer Datenbank)
	Überwachung Erfolgreich	Eine Aktion wurde ausgeführt, welche mit dem Attribut »Erfolgreich« ausgestattet ist.
	Überwachung Fehlversuch	Eine Aktion wurde ausgeführt, welche mit dem Attribut »Fehlschlag« ausgestattet ist.

3.5.5 Beispiele für Meldungen der Ereignisanzeige

Nachfolgend werden Beispiele für verschiedene Meldungen der Ereignisanzeige gezeigt. Die Abbildungen dokumentieren den Aufbau und den Informationsgehalt verschiedener Meldungen. Diese Detailansichten sind durch einen Doppelklick auf den entsprechenden Fehler zu erreichen.

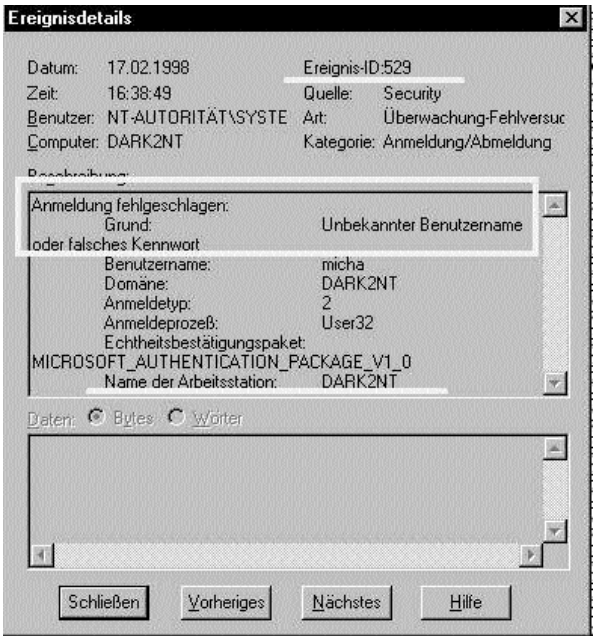


Abbildung 45: Meldung 529: Falsches Login

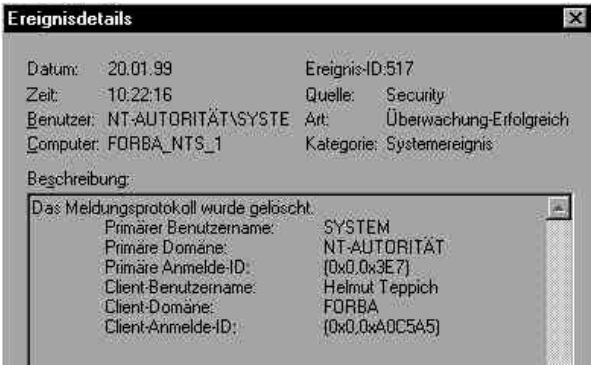


Abbildung 46: Meldung 517: Löschung der Ereignisanzeige

Die Meldungen sind nur schwer zu lesen, wenn sie nicht zum täglichen Arbeitsumfeld gehören. Wichtig für die Interessenvertretung ist unseres Erachtens die Kenntnis, welche Meldungsnummern es gibt und wo sie und eine Erläuterung zu erhalten sind.

Eine ausführliche Liste aller Fehlercodes ist u. a. auf der CD zum Buch »Technische Referenz Windows NT Resource Kit 4.0« in den Dateien »Ntmsgs.hlp« und »Auditcat.hlp« beschrieben. Zu finden sind diese Dateien auf der CD unter Online Docs/ Windows NT Messages. Die beschriebenen Event Logs reichen von 512 bis 9507.

Die »Technische Referenz« gehört zum Standardwerkzeug jedes Administrators, so daß davon auszugehen ist, daß diese Bücher (es sind 4 Stück) und die CD im Betrieb vorhanden sind.

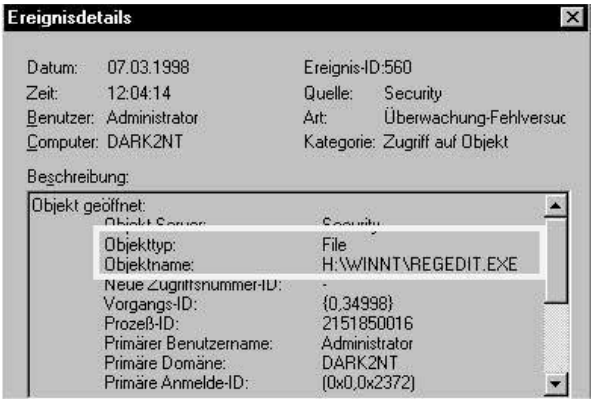


Abbildung 47: Richtlinienänderung: Benutzerrecht Systemzeit gesetzt

Abbildung 48: Kontenverwaltung neues Benutzerkonto

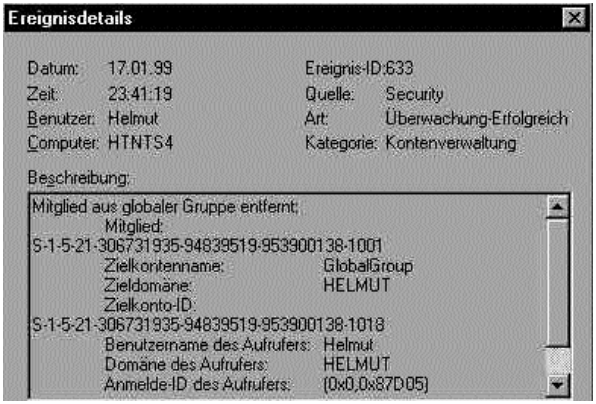


Abbildung 49: Mitglied aus globaler Gruppe entfernt

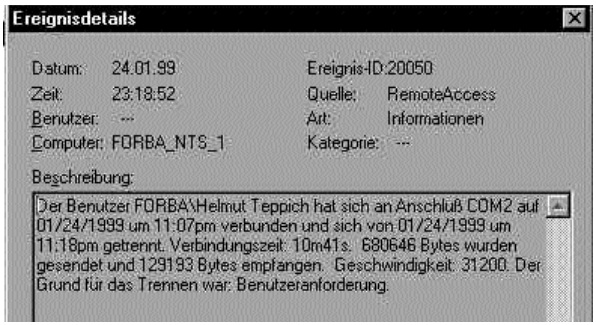


Abbildung 50: RAS-Abmeldung

In vielen Meldungen wird nicht der Name im Klartext, sondern nur die SID angezeigt. Diese läßt sich für lokale Anmeldungen in der Registry des jeweiligen Rechners unter HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft\WindowsNT \CurrentVersion\Profile-

LIst \<SID> ProfileImagePath anzeigen. Im Internet werden die Freeware-Programme sid2user bzw. user2sid angeboten, die jede SID und jeden User identifizieren.

3.5.6 Meldungen der Ereignisanzeige (EventLog)

In den drei Ereignisprotokollen werden – soweit eingerichtet – unzählige Ereignisse, die Windows NT-Aktionen und -Reaktionen widerspiegeln, protokolliert. Dazu kommen noch die Ereigniseinträge anderer Programme, die ihre Ereignisse ausschließlich in das Anwendungsprotokoll schreiben.

Nachfolgend sind einige Ereignisse aufgeführt, deren Vorfall Anlaß zur Nachprüfung geben kann.

Aktion	**Meldungs-Nr.**
System neu gestartet	512
System heruntergefahren	513
Ereignisanzeige gelöscht	517
Unbekannter Benutzer oder falsches Paßwort	529
Erfolgloser Login – Zugriffsversuch außerhalb der zulässigen Zeiten	530
Erfolgloser Login über ein deaktiviertes Konto	531
Erfolgloser Login – Kontoberechtigung abgelaufen	532
Erfolgloser Login – Benutzer darf sich nicht an diesem Computer anmelden	533
Erfolgloser Login – Paßwort abgelaufen	535
Erfolgloser Login	537
Erfolgreiches Logout	538
Erfolgloser Login – Konto gesperrt	539
Zugriff auf Objekt (Datei, Drucker etc.)	560
Richtlinienänderung – Benutzerrechte zugeteilt	608
Richtlinienänderung – Benutzerrechte entfernt	609
Benutzerrecht wurde gesperrt	609
Richtlinienänderung – Neue vertraute Domäne	610
Richtlinienänderung – Vertraute Domäne entfernt	611
Änderung d. Überwachungsrichtlinien	612
Benutzer-Konto wurde angelegt	624
Benutzerkonto Typ geändert (lokal <-> serverbasiert	625

Benutzerkonto geöffnet	626
Benutzer-Paßwort wurde gesetzt	628
Benutzer-Konto wurde gesperrt	629
Benutzer gelöscht	630
Globale Gruppe – Neue Gruppe	631
Globale Gruppe – Mitglied hinzugefügt	632
Globale Gruppe –	633
Globale Gruppe – Gruppe gelöscht	634
Lokale Gruppe – Neue Gruppe	635
Lokale Gruppe – Mitglied hinzugefügt	636
Lokale Gruppe – Mitglied entfernt	637
Lokale Gruppe – Gruppe gelöscht	638
Benutzer-Konto geändert	642
Benutzer-Konto wurde geändert	642
Serverbasiertes Profil – Benutzer wurde obligatorisches Profil zugewiesen	1002
Serverbasiertes Profil – Das obligatorische Profil wurde nicht gefunden	1003
Serverbasiertes Profil – Update von diesem Rechner nicht erlaubt	1018
Benutzer konnte sich in der RAS-Verbindung nicht authentisieren	20016
Benutzer hat sich erfolgreich über RAS angemeldet	20017
Benutzer X an Anschluß Y wurde unter der Nummer 1234567 zurückgerufen.	20068
Rückrufversuch des RAS-Servers ist fehlgeschlagen	20093

Eine Liste der möglichen Ereignisse ist im Microsoft Windows NT Resource Kit 4.0 unter *Online Docs* in der Hilfedatei *Windows NT Messages* aufgezeigt.

3.5.7 NT-eigene Werkzeuge zur Informationssammlung

Bei der administrativen Arbeit mit Windows NT wird neben den graphischen Werkzeugen häufig auf kommandozeilenorientierte Befehle zurückgegriffen. Diese ermöglichen zum Teil eine effizientere Arbeitsweise und verkürzen bei geschickter Anwendung den Lösungsweg erheblich. Die Kommandozeilenbefehle können auch von der Interessenvertretung zur Analyse genutzt werden. Eines der am häufigsten eingesetzten Werkzeuge ist der Befehl NET. Die NET.EXE Datei

ist im Verzeichnis WINNTsystem32 zu finden, kann aber aus jeder Eingabeaufforderung ohne spezielle Pfadangabe aufgerufen werden.

3.5.7.1 Die NET-Befehle

Mit Hilfe des Kommandos NET können viele Einstellungen in der Eingabeaufforderung erfolgen, ohne graphische Hilfsmittel zu benutzen. So können mit dem NET-Befehl Benutzer oder Gruppen eingerichtet werden, Ressourcen freigegeben werden oder Einstellungen am System vorgenommen werden, wie zum Beispiel die Richtlinien für Benutzerkennworte.

Auf die Frage, wieso diese Aufgaben nicht mit Hilfe der graphischen Tools erledigt werden, kann mit einem Beispiel geantwortet werden. Die Einrichtung von einhundert oder mehr Benutzern kann mit Hilfe der Kommandozeilenbefehle in einer Stapelverarbeitungsdatei geschehen. Dadurch wird die Aufgabe weitgehend automatisiert, was bei dem graphischen Benutzermanager nicht möglich ist.

Der Befehl NET bietet weiterhin die Möglichkeit, nur Informationen zu einem Themengebiet anzuzeigen. So kann der Aufruf *net localgroup* genutzt werden, um sich alle lokalen Gruppen des Windows NT-Systems anzeigen zu lassen.

Im folgenden werden einige Grundparameter des Net-Befehls tabellarisch gezeigt. Um die genaue Syntax der einzelnen Befehle zu erfahren, ist folgendes einzugeben: *net help* Grundparameter, z. B. *net help accounts.*

Kommando	**Erklärung**
Net accounts	aktualisiert die Benutzerdatenbank und ändert Anmelde- und Kennwortbedingungen ohne Parameter: aktuelle Einstellungen
Net computer	fügt Rechner in die Domänendatenbank nur auf Windows NT Server verfügbar
Net config server|workstation	zeigt Konfigurationsinformationen des Arbeitsstations- oder Serverdienstes an
Net group	fügt globale Gruppen auf dem Server hinzu, zeigt sie an und ändert sie ohne Parameter: Gruppennamen auf dem Server werden angezeigt

Net localgroup	ändert lokale Gruppen auf dem Rechner ohne Parameter: zeigt Servernamen und Namen der lokalen Gruppen auf dem Rechner an
Net pause	unterbricht einen Windows NT-Dienst oder den Zugriff auf eine Ressource
Net print	zeigt Druckaufträge und Druckerwarteschlange an
Net session	zeigt die Sitzungen des Computers mit anderen Computern an oder beendet sie ohne Parameter: Sitzungsinformationen des aktuellen Rechners
Net share	stellt die Ressourcen eines Servers den Netzwerkbenutzern zur Verfügung ohne Parameter: Informationen über alle auf dem Rechner freigegebenen Ressourcen werden angezeigt
Net start	listet aktive Dienste auf
Net statistics workstation|server	zeigt das Statistikprotokoll für den angegebenen Server- oder Arbeitsstationsdienst an ohne Parameter: es werden die aktiven Dienste aufgelistet mit der dazugehörigen Statistik
Net use	verbindet einen Rechner mit einer freigegebenen Ressource oder beendet diese Verbindung ohne Parameter: eine Liste der Netzwerkverbindungen wird angezeigt
Net user	fügt Benutzerkonten hinzu, löscht oder ändert diese ohne Parameter: Liste aller Benutzerkonten auf dem Rechner
Net view	zeigt eine Liste der Rechner oder der von einem Rechner freigegebenen Ressourcen an

Beispielscript für die Anwendung der NET-Befehle

Wie der Funktionsumfang der NET-Befehle auch im Rahmen einer automatisch im Hintergrund laufenden Abfrage umgesetzt werden kann, zeigt die folgende Batchdatei:

```
@echo off
rem Beispieldatei WNTINFO.BAT von Michael Kürschner
rem Auf Basis einer Idee aus Tom Sheldon's Buch
rem »WindowsNT Security Handbook Security«
rem
rem eigenen Pfad hinter Variable PFAD schreiben
SET PFAD=h:\temp
rem entsprechenden Namen des Rechners hinter Variable RECHNERNAME
rem schreiben
SET RECHNERNAME=dark2nt
echo ————————————————————————————————- >> %PFAD%\report.txt
echo Informationen zu Ihrem Windows NT System >> %PFAD%\report.txt
echo ————————————————————————————————- >> %PFAD%\report.txt
echo Letzter Durchlauf >> %PFAD%\report.txt
echo.|date >> %PFAD%\report.txt
echo.|time >> %PFAD%\report.txt
echo —- Bestehende Benutzerkonten —- >> %PFAD%\report.txt
net user >> %PFAD%\report.txt
echo ********************************** >> %PFAD%\report.txt
echo —- Globale Gruppen—- >> %PFAD%\report.txt
net group >> %PFAD%\report.txt
echo ********************************** >> %PFAD%\report.txt
echo —- Vorhandene lokale Gruppen —- >> %PFAD%\report.txt
net localgroup >> %PFAD%\report.txt
echo ********************************** >> %PFAD%\report.txt
echo —- Einstellungen der Kennwortrichtlinien —- >> %PFAD%\report.txt
net accounts >> %PFAD%\report.txt
echo ********************************** >> %PFAD%\report.txt
echo —- Systemfreigaben —- >> %PFAD%\report.txt
net share >> %PFAD%\report.txt
echo ********************************** >> %PFAD%\report.txt
echo —-Freigegebene Ressourcen —- >> %PFAD%\report.txt
net view \\%RECHNERNAME% >> %PFAD%\report.txt
```

```
echo ************************************      >> %PFAD%\report.txt
echo —-Freigegebene Ressourcen in Benutzung—-  >> %PFAD%\report.txt
net use \\%RECHNERNAME%                        >> %PFAD%\report.txt
echo ************************************      >> %PFAD%\report.txt
echo —-Aktive Sitzung—-                        >> %PFAD%\report.txt
net session \\%RECHNERNAME%                    >> %PFAD%\report.txt
echo ************************************      >> %PFAD%\report.txt
echo —-SERVER KONFIGURATION—-                  >> %PFAD%\report.txt
net config server                              >> %PFAD%\report.txt
echo ************************************      >> %PFAD%\report.txt
echo —-WORKSTATION KONFIGURATION—-             >> %PFAD%\report.txt
net config workstation                         >> %PFAD%\report.txt
echo ************************************      >> %PFAD%\report.txt
echo —-SERVER STATISTICS—-                     >> %PFAD%\report.txt
net statistics server                          >> %PFAD%\report.txt
echo ************************************      >> %PFAD%\report.txt
echo —-WORKSTATION STATISTICS—-                >> %PFAD%\report.txt
net statistics workstation                     >> %PFAD%\report.txt
echo ************************************      >> %PFAD%\report.txt
echo ENDE DER DATEI                            >> %PFAD%\report.txt
```

Die vorstehende Batchdatei erzeugt im angegebenen Pfad eine Datei namens report.txt. Bei einem neuen Durchlauf werden die neu gewonnenen Informationen an die bestehende Datei report.txt angehängt.

Die Variablen PFAD und RECHNERNAME sind den aktuellen Gegebenheiten anzupassen, um Fehler bei der Ausführung zu vermeiden.

Das Ergebnis in der Datei report.txt sieht so aus:

```
————————————————————————————————
 Informationen zu Ihrem Windows NT System
————————————————————————————————
Letzter Durchlauf
Aktuelles Datum: Mo 20.0
7.1998
Geben Sie das neue Datum ein: (TT-MM-JJ)
Aktuelle Zeit: 18:28:03,93
Geben Sie die neue Zeit ein:
—-Bestehende Benutzerkonten—-
Benutzerkonten für \\DARK2NT
————————————————————————————————————————
Administrator                gaeste                Micha
Replikator                   testnutzer
************************************
—-Globale Gruppen—-
************************************
—-Vorhandene lokale Gruppen—-
Gruppen für \\DARK2NT
————————————————————————————————————————-
*Administratoren             *Arbeitsgruppe        *Benutzer
*Gäste                       *Hauptbenutzer        *Replikations-Operator
*Sicherungs-Operatoren
************************************
—-Einstellungen der Kennwortrichtlinien—-
Abmelden erzwingen nach :                          Nie
Minimales Kennwortalter (Tage):                    0
Maximales Kennwortalter (Tage) :                   Unbegrenzt
Minimale Kennwortlänge :                           5
Länge der Kennwortchronik :                        Keine
Sperrschwelle:                                     4
Sperrdauer (Minuten):                              Nie
Lockout observation window (Minuten):              30
Rolle des Computers:                               SERVER
```

```
************************************
—-Systemfreigaben—-
Name                 Ressource                        Beschreibung
———————————————————————————————————-
F$                   F:\                              Standardfreigabe
IPC$                                                  Remote-IPC
G$                   G:\                              Standardfreigabe
C$                   C:\                              Standardfreigabe
D$                   D:\                              Standardfreigabe
E$                   E:\                              Standardfreigabe
ADMIN$               H:\WINNT                         Remote-Admin
H$                   H:\                              Standardfreigabe
print$               H:\WINNT\system32\spool\drivers   Druckertreiber
I$                   I:\                              Standardfreigabe
Stuff                E:\Stuff                         HPDeskJet 690C
************************************
—-Freigegebene Ressourcen—-
Freigegebene Ressourcen auf \\dark2nt
Name                 Typ          Lokal               Beschreibung
———————————————————————————————————-
HPDeskJet 690C
                     Drucker                          HP DeskJet 660C
Stuff                Platte
************************************
—-Freigegebene Ressourcen in Benutzung—-
************************************
—-Aktive Sitzung—-
Benutzername         Administrator
Computer             DARK2NT
Gastanmeldung        Nein
Client-Typ           Windows NT 1381
Sitzungszeit         00:00:00
Ruhezeit             00:00:00
```

```
Name            Typ                         Öffnungen
-------------------------------------------------------------------------------
IPC$            IPC
************************************
---SERVER KONFIGURATION---
Server-Name                                 \\DARK2NT
Server-Beschreibung
Software-Version                            Windows NT 4.0
Server ist aktiv auf                        NetBT_Elnk31
Unsichtbarer Server                         Nein
Max. angemeldete Benutzer                   Unbegrenzt
Max. offene Dateien pro Sitzung             2048
Sitzungsruhezeit (Min)                      15
************************************
---WORKSTATION KONFIGURATION---
Computer-Name                               \\DARK2NT
Benutzername                                Administrator
Arbeitsstation aktiv an                     NetBT_Elnk31 (0020AFC8E1D3)
Software-Version                            Windows NT 4.0
Arbeitsstationsdomäne                       WORKGROUP
Anmeldedomäne                               DARK2NT
COM offen; Zeitüberschreitung (s)           3600
COM gesendete Anzahl (Bytes)                16
COM senden; Zeitüberschreitung (ms)         250
************************************
---SERVER STATISTICS---
Server-Statistik für \\DARK2NT
Statistik seit
7/20/98 6:18 PM
Akzeptierte Sitzungen                       1
Timeout-Sitzungen                           0
Sitzungsabbruch wegen Fehler                0
Kilobytes gesendet                          1
Kilobytes empfangen                         1
Mittlere Antwortzeit (ms)                   0
```

Systemfehler	0
Berechtigungsverstî·e	0
Kennwortverstî·e	0
Dateizugriffe	0
DFö-Hardware-Zugriffe	0
Gespeicherte Druckaufträge	0
Anzahl Pufferüberläufe	
Gro·e Puffer	0
Anfrage-Puffer	0

****

—-WORKSTATION STATISTICS—-

Arbeitsstationsstatistik für \\DARK2NT

Statistik seit

7’20’98 6:18 PM

Kilobytes empfangen	512
SMBs (Server Message Blocks) empfangen	5
Bytes übertragen	923
SMBs (Server Message Blocks) übertragen	5
Lesevorgänge	0
Schreibvorgänge	21
Verweigerte Rohdaten-Lesevorgänge	0
Verweigerte Rohdaten-Schreibvorgänge	0
Netzwerkfehler	0
Verbindungen hergestellt	2
Verbindungen wiederhergestellt	0
Server-Trennungen	0
Gestartete Sitzungen	2
Aufgehängte Sitzungen	0
Gescheiterte Sitzungen	0
Gescheiterte Vorgänge	0
Erfolgreiche Benutzung	1
Gescheiterte Benutzung	0

****

ENDE DER DATEI

Für eine regelmäßige Ausführung der Beispieldatei WNTINFO.BAT bietet Windows NT den Dienst »Scheduler« an. Mit dem Scheduler lassen sich Programme zeitgesteuert aufrufen. Das Recht, den Scheduler einzusetzen, haben standardmäßig nur die Administratoren. Damit die Batchdatei regelmäßig ausgeführt werden kann, ist ein Job zu definieren. Für zeitgesteuerte Befehle hat Windows NT das Kommandozeilen-Programm AT.EXE.

Damit die Batchdatei WNTINFO.BAT an jedem 5., 10., 15., 20., 25. und 30. des Monats um 17:00 Uhr ausgeführt wird, ist in der Eingabeaufforderung das Kommando:

```
at 17:00 every: 5, 10, 15, 20, 25, 30 WNTINFO.BAT
```

einzugeben. Bei einer erfolgreichen Ausführung wird eine Job-ID ausgegeben.

4 UMSETZUNG DER DATENSCHUTZRECHTLICHEN VORGABEN DES § 9 BDSG

In diesem Abschnitt wird geprüft, ob und wie die gesetzlichen Bestimmungen des § 9 BDSG beim Umgang mit personenbezogenen Daten in einer Windows NT-Umgebung verwirklicht werden können, ohne zusätzliche Software oder Hardware einzubinden. Der § 9 und die Anlage zu § 9 Satz 1 BDSG regeln die technischen und organisatorischen Maßnahmen bei der Verarbeitung personenbezogener Daten. Die Anwendung der Vorgaben sind oft Gegenstand der Verhandlungen bei Anwendung von EDV-Systemen und der Einhaltung des Datenschutzes, den die Interessenvertretungen im Rahmen ihrer allgemeinen Aufgaben wahrzunehmen haben.

§ 9 »Technische und organisatorische Maßnahmen«

»Öffentliche und nichtöffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind die Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzaufwand steht.«

Entsprechend der Anlage zu § 9 Satz 1 sind bei der Verarbeitung personenbezogener Daten folgende technischen und organisatorischen Maßnahmen zu ergreifen:

»Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind:

»1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle).«

Um den Zugriff auf das Windows NT-System kontrollieren zu können, muß eine benutzerspezifische Anmeldung mit einer Paßwortabfrage eingerichtet werden. Außerdem ist das Paßwort in zyklischen Abständen durch ein neues zu ersetzen (siehe Abschnitt 2.5.1). Um ein unbefugtes Eindringen oder den Versuch des Eindringens in das Windows NT-System aufzudecken, ist die Ereignisanzeige zu archivieren und regelmäßig auf fehlgeschlagene Anmeldeprozeduren hin zu überprüfen.

Gegen den physischen Zugriff auf Tastatur, Bildschirm und Rechner müssen diese Teile in ständig verschlossenen Räumen untergebracht sein.

Eine Zugangskontrolle läßt sich mit Windows NT realisieren.

»2. zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle).«

Das Entfernen eines Datenträgers, sprich einer Festplatte, zu verhindern, ist nur durch bauliche Maßnahmen zu sichern.

Hingegen kann mit dem Dateisystem NTFS gesichert werden, daß nur befugte Personen den Datenträger lesen, kopieren und ändern dürfen. Verzeichnisse und Dateien sind mit differenzierten Berechtigungen zu versehen. Durch die Organisation in Gruppen können zugriffsberechtigte Benutzer von den restlichen abgetrennt werden, indem letzteren das Recht »Kein Zugriff« gegeben wird. Dadurch haben diese Personen keinen Zugriff auf die Verzeichnisse und Daten. Die Herangehensweise ist im Abschnitt »NTFS und Zugriffsrechte« (siehe Abschnitt 2.7) und den anschließenden Unterkapiteln beschrieben.

Eine Datenträgerkontrolle läßt sich mit Windows NT realisieren.

»3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle).«

Um eine unbefugte Eingabe zu verhindern, dürfen nur NTFS-Laufwerke auf dem Rechner vorhanden sein, Verzeichnisse und Dateien sind mit differenzierten Berechtigungen zu versehen. Durch die Organisation in Gruppen können zugriffsberechtigte Benutzer von den restlichen abgetrennt werden. indem Letzteren das Recht »Kein Zugriff« gegeben wird. Dadurch haben diese Personen keinen Zugriff auf die Verzeichnisse und Daten. Weiterhin sind die entsprechenden Laufwerke, Verzeichnisse und Dateien zu überwachen (siehe Abschitt 3.5.1). Mit diesem Schritt kann nachvollzogen werden, welche Benutzerkonten auf die personenbezogenen Dateien zugegriffen haben.

Eine Speicherkontrolle läßt sich mit Windows NT auf der Verzeichnis- und Dateiebene realisieren. Welche Verarbeitungen innerhalb einer Datei stattfinden, muß von anderen Programmen gewährleistet werden.

»4. zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle).«

Die Erfüllung dieser Forderung kann erreicht werden, indem auf den Rechner kein Zugriff über Modem/ISDN mittels RAS möglich ist. Dazu müssen die entsprechenden RAS-Dienste unter START – EINSTELLUNGEN – DIENSTE abgeschaltet werden.

Falls dennoch eine RAS-Verbindung auf dem Rechner notwendig sein sollte, sind die Berechtigungen restriktiv zu vergeben (siehe Abschnitt 2.4.2 und RAS [Remote Access Service]). RAS-berechtigte Benutzer müßten dazu ein gesondertes Konto (z. B. RAS Hans Meier) erhalten. Dieses Konto dürfte dann auch nicht Mitglied in lokalen Gruppen mit Zugang zu personenbezogenen Daten werden. RAS-Konten müssen zu lokalen Gruppen zusammengefaßt werden. Diesen Gruppen müßten auf Verzeichnisse und Dateien mit personenbezogenen Daten explizit das Recht »Kein Zugriff« erhalten.

Eine Benutzerkontrolle läßt sich mit Windows NT nur bedingt realisieren.

»5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle).«

Um dieser Forderung nachzukommen, dürfen personenbezogene Daten nur auf reinen NTFS-formatierten Laufwerken (keine DOS-Partition) gespeichert werden. Auf die sensiblen Dateien und Verzeichnisse sind NTFS-Zugriffsrechte für berechtigte Gruppen zu vergeben. Alle anderen Gruppen, die keinen Zugriff auf diese Verzeichnisse und Dateien erhalten sollen, müßten explizit das Recht »Kein Zugriff« erhalten. Damit erhalten nur die Benutzer, die ausschließlich Mitglieder der berechtigten Gruppen sind, Zugang zu den gespeicherten Daten.

Eine Zugriffskontrolle läßt sich mit Windows NT realisieren.

»6. zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle).«

Eine Kontrolle, ob die übertragenen Daten nur bei der definierten Stelle ankommen und wohin sie übertragen wurden, läßt sich ohne zusätzliche Hilfsmittel nur schwer feststellen. Bei einer Überwachung der Dateien kann nur festgestellt werden, daß die

Datei gelesen wurde, jedoch nicht, ob diese kopiert wurde und auch nicht wohin. Für diese geforderte Maßnahme bietet Windows NT keine eigene Lösung.

Eine Übermittlungskontrolle läßt sich mit Windows NT nicht realisieren.

»7. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle).«

Bei der Überwachung von Dateien kann festgestellt werden, zu welchem Zeitpunkt von wem eine Datei verändert wurde. Die Ereignisanzeige zeigt jedoch nicht an, ob und welche Daten in einer Datei oder Datenbank verändert wurden. Diese Aufgabe muß durch die Software, mit der die Daten gepflegt werden, erfüllt werden. Diese Problematik haben aber Sicherheitsprogramme von Drittanbietern, da sie Dateien immer nur »von außen« überwachen können.

Eine Eingabekontrolle läßt sich mit Windows NT nur bedingt realisieren.

»8. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle).«

Die Erfüllung dieser Anforderung ist durch die Einrichtung einer speziellen Gruppe teilweise möglich. Nur die Mitglieder dieser Gruppe dürfen auf die zu verarbeitenden Dateien zugreifen, für alle anderen müßte das Recht auf »Kein Zugriff« gesetzt werden. Die Dateien sind zu überwachen. Mit diesen Mitteln kann in der Ereignisanzeige überprüft werden, wann diese Dateien durch welches Konto wie verarbeitet wurden (Lesen, Schreiben, Umbenennen, Kopieren). Was innerhalb einer Datei passiert, ist mit Windows NT-eigenen Mitteln nicht nachzuvollziehen.

Eine Eingabekontrolle läßt sich mit Windows NT nur bedingt realisieren.

»9. zu verhindern, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle).«

Diese Maßnahme ist mit vorhandenen Mitteln in Windows NT nicht zu erfüllen. Für diesen Fall muß auf Software von Drittanbietern zurückgegriffen werden, welche die relevanten Dateien beim Speichern auf einem Speichermedium verschlüsselt. Mit dieser Methode kann sichergestellt werden, daß die Daten nicht von einer anderen Person gelesen werden können. Das gleiche gilt für die Übertragung von Daten über ein Netzwerk. Diese Daten sind ebenfalls mit einem Produkt eines Drittanbieters vor dem Versenden zu verschlüsseln.

Eine Transportkontrolle läßt sich mit Windows NT nicht realisieren.

»10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).«

Hier sind organisatorische Maßnahmen notwendig.

Eine Organisationskontrolle läßt sich mit Windows NT nicht realisieren.

Als Ergebnis läßt sich festhalten, daß Windows NT in der Lage ist, mit den eigenen Werkzeugen einen gewissen Datenschutz zu gewährleisten. Die Grundfunktionalitäten reichen unseres Erachtens aus, um betriebsintern eine datenschutzmäßig sichere Datenverarbeitung durchzuführen. Bei einer Anbindung an das Internet oder großen WANs (überregionalen Netzen) ist der Einsatz von Zusatzprodukten (z. B. Verschlüsselungsprogramme) zur Gewährleistung des Datenschutzes notwendig.

5 WINDOWS NT – EINE MITBESTIMMUNGSPFLICHTIGE TECHNISCHE EINRICHTUNG

Die Mitbestimmung der Interessenvertretung gemäß BetrVG und PersVG liegt vor, wenn

- eine technische Einrichtung installiert ist,
- die dazu geeignet ist,
- Leistung und Verhalten von Arbeitnehmern zu überwachen und zu kontrollieren.

Diese Ansicht des Bundesarbeitsgerichtes hat sich bis heute nicht geändert, und alle Urteile zur Anwendung von technischen Einrichtungen bestätigen diese drei Punkte immer wieder.

Windows NT, als Server wie als Workstation,

- sind zweifelsfrei technische Einrichtungen,
- die in den systemeigenen Funktionalitäten die Möglichkeit bieten,
- das Verhalten von Arbeitnehmern zu überwachen und zu kontrollieren.

Die Überwachung ist leicht, schnell und ohne daß die überwachte Person es wahrnimmt, durchführbar.

Durch die Möglichkeit, differenzierte Rechte auf nahezu allen Ebenen der täglichen Arbeit im System zu vergeben, können alle Tätigkeiten, die Zugriffe auf Objekte (Laufwerke, Verzeichnisse, Dateien, Drucker, Registry) darstellen, ständig der Prüfung und gegebenenfalls der Protokollierung unterzogen werden.

Windows NT ist daher unabhängig von den eingesetzten Anwendungsprogrammen als mitbestimmungspflichtig im Sinne des § 87 Abs.1 Ziffer 6 BetrVG bzw. der entsprechenden Paragraphen in den PersVG anzusehen.

6 WINDOWS NT 5 – WINDOWS 2000

Microsoft plant seit längerem, Windows NT Version 4 durch eine neue Version 5 zu ersetzen. Inzwischen wurde auch der Name Windows NT aufgegeben und durch Windows 2000 ersetzt. Nachdem der Einführungstermin von W2K (wie die amerikanische Abkürzung lautet) nach und nach ins Jahr 2000 gerutscht ist, wird auch deutlicher, was den Kunden mit Windows NT 5 erwartet:

Die gesamte Organisation der bestehenden Netzstruktur muß bei Einführung von Windows 2000 vollkommen neu überarbeitet werden.

Microsoft hat die Kritik an dem mangelhaften Verzeichnisdienst, die umständliche Domänenstruktur und die Kritik an den Sicherheitsstandards in ein komplett neues Produkt umgesetzt. Bisher existieren nur sogenannte BETA-Versionen des neuen Produkts, aktuell ist die 3. BETA-Version (Build 2031) zum Test an ausgewählte Firmen und Personen freigegeben. BETA-Versionen sind keine Endversionen, und in der EDV-Branche hat sich immer wieder gezeigt, daß das Endprodukt noch einmal ganz anders aussieht als vorher vermutet wurde.

Die in vielen Zeitschriften und Büchern (siehe z. B. Martin Kuppinger: Windows 2000) vorgestellten neuen Funktionen wie MMC (Management Console), SCE (Security Configuration Editor), AD (Active Directory) usw. haben den praktischen Einsatz noch vor sich.

Aus den uns zur Zeit vorliegenden Microsoft-Beschreibungen, Kommentierungen in Zeitschriften, im Internet und in ersten Büchern geht immer wieder hervor, daß die Anwendung von Windows 2000 ein vollkommenes Umdenken, Umorganisieren und Lernen in den EDV-Abteilungen, im Management, bei den Datenschutzbeauftragten und damit auch bei den Interessenvertretungen und den Belegschaften erfordert.

Vor diesem Hintergrund wurde auf eine Vertiefung dieses Themas verzichtet, da Spekulationen über eventuelle Handlungsnotwendigkeiten in einem zukünftigen Windows 2000-System unserer Ansicht nach keine Orientierung für die Arbeit einer Interessenvertretung sein sollte.

7 NÜTZLICHE PROGRAMME ZUR BEGEHUNG, KONTROLLE UND ADMINISTRATION VON WINDOWS NT

Im folgenden werden einige – subjektiv ausgewählte – Programme, die in der eigenen Tagesarbeit Anwendung finden, kurz vorgestellt. Alle Programme lassen sich als Shareware aus dem Internet kostenlos beziehen. Sie können unseres Erachtens Hilfsmittel bei einer Begehung oder Kontrolle durch die Interessenvertretung sein (die Programme passen jedes für sich auf eine Diskette) und können auch für Administratoren oder Revisoren interessante Werkzeuge sein.

7.1 ELWIZ (EVENTLOG WIZARD) 2.03

email fh@heysoft.de
Homepage: http://www.heysoft.de/

Beschreibung des Programmierers

ELWIZ ist ein komfortables Werkzeug zur Verwaltung und automatischen Speicherung der Ereignisanzeigen. Sofern der mitgelieferte Dienst »Event-Watcher« installiert wird, können die Ereignisprotokolle getrennt nach Protokoll und Monat in vordefinierten Verzeichnissen archiviert werden. Die aktuellen Protokolle und die archivierten Protokolle stehen gleichzeitig für die Auswertung zur Verfügung.

Die Ereignisprotokolle werden nach folgendem Schema archiviert:

yyyy_mm_machine_type.evt

wobei:	yyyy	–	Jahr
	mm	–	Monat
	machine	–	Maschinenname
	type	–	Eventlog art

ist.

Der Sicherheitslog von Server1 vom Januar 1999 erhält dann den Namen:

1999_01_Server1_Security.evt

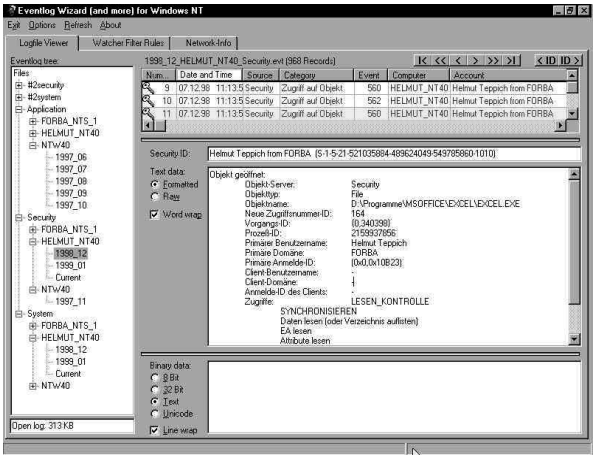


Abbildung 51: ELWIZ

7.2 DUMPACL (V2.81b)

Homepage: http://www.somarsoft.com.

Beschreibung des Programmierers

Somarsoft DumpAcl-NT ist ein Sicherheitsüberwachungsprogramm für Windows NT. Es ermöglicht, die vergebenen Rechte an Verzeichnissen, Dateien und der Registry, die Überwachungseinstellungen, Benutzer- und Gruppen-Informationen aus den Zugriffskontrollisten (ACL) auszulesen und in eine lesbare Form zu bringen, um damit Sicherheitslöcher in der Systemsicherheit aufzudecken.

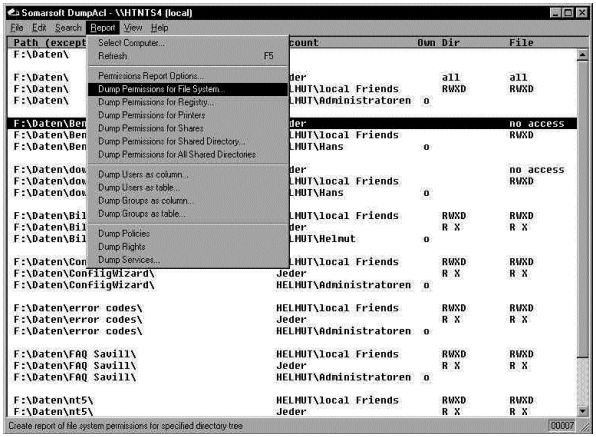


Abbildung 52: DumpACL

7.3 EVENTLIST – ZUSAMMENFASSUNG VON EVENTDATEIEN, VERSION 2.8

Homepage: http://www.heysoft.de/

Beschreibung des Programmierers

Das Programm EventList ist ein Programm aus dem Paket der Kommandozeilenprogramme »Report Event für Windows NT«. Es listet für alle (die Vollversion auch für eine oder einen Teil der) Eventlog-Dateien eines Verzeichnisses die darin vorkommenden Ereignisse und deren Anzahl auf. Das Programm läuft nur unter Windows NT. Es ist sowohl als englische als auch als deutsche Version erhältlich.

Momentan gehören folgende Module zu »Report Event für Windows NT«:

EventList	Zusammenfassung über eine oder mehrere Logdateien
EventSave+	Arbeitet wie EventSave, es lassen sich aber einzelne Logdateien auswählen
EventCopy	Arbeitet wie EventSave, löscht aber die Logs nicht

R20050	Auswertung der RAS-Event 20050 bzw. 20048 (RAS-Anrufe)
RP10	Auswertung des Print-Event 10 (Printjobs)
R528	Auswertung der Events 528 und 538 des Sicherheits-Logs (Dauer und Anzahl von Nutzersitzungen)
R529	Auswertung des Events 529 des Sicherheits-Logs (fehlgeschlagenes Einloggen)
R592	Auswertung der Events 592 und 593 des Sicherheits-Logs (Softwarenutzung)

7.4 SICHERHEITSMANAGER 2.02 FÜR WINDOWS NT 4.0

Homepage: http://home.t-online.de/home/wispro/secumgr.htm

Beschreibung des Programmierers

Der Sicherheitsmanager ermöglicht es, die Sicherheitseinstellungen von Verzeichnissen und Dateien auf einer NTFS-Partition schnell zu überblicken und auch zu ändern. Während der Dateimanager oder der Windows-Explorer die Sicherheitseinstellungen nur auf Befehl und nur für die ausgewählte Datei oder Verzeichnis anzeigt, stellt der Sicherheitsmanager diese Informationen sofort für alle Dateien eines Verzeichnisses oder sogar für einen ganzen Verzeichnisbaum zur Verfügung.

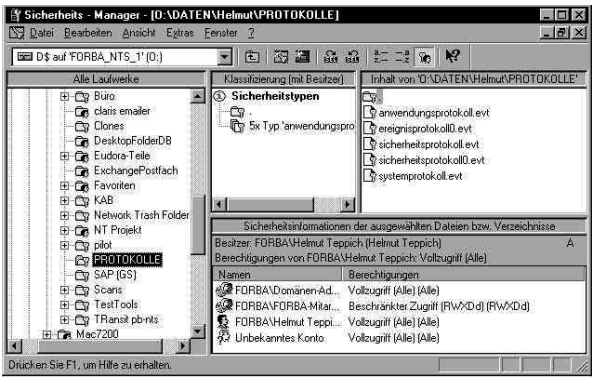


Abbildung 53: Symbole im Sicherheits-Manager

Das Programm hat die Möglichkeit, insgesamt acht ausgewählte Berechtigungen (z. B. JEDER mit Vollzugriff oder Meier) farblich zu kennzeichnen. Beim Bewegen der Maus über das Fenster wird beim Vorliegen dieser Berechtigung jedesmal die ausgewählte Farbe, z. B. Rot, angezeigt. Auf diese Weise lassen sich auch große Laufwerke nach Sicherheitslöchern durchsuchen.

Darstellung von Sicherheitsinformationen

Der Sicherheitsmanager benutzt mehrere Techniken, um die Sicherheitsinformationen übersichtlich und dennoch bei Bedarf detailliert darzustellen:

+ Für jedes Verzeichnis und jede Datei wird durch ein überlagertes Symbol angezeigt, welche Berechtigungen Sie haben:

	Sie sind der Besitzer
	Sie haben Vollzugriff auf die Sicherheitseinstellungen
	Sie dürfen den Inhalt dieses Verzeichnisses bzw. Datei ändern (aber nicht die Sicherheitseinstellungen)
	Sie dürfen dieses Verzeichnis anzeigen bzw. diese Datei lesen
	Sie haben keine Berechtigung auf dieses Verzeichnis bzw. diese Datei zuzugreifen
	Dieses Verzeichnis bzw. diese Datei ist durch einen anderen Prozeß gesperrt

+ Im Sicherheitsinformationsfenster wird der Besitzer und die Berechtigungsliste der ausgewählten Dateien bzw. Verzeichnisse angezeigt
+ Im Klassifizierungsfenster werden Verzeichnisse und Dateien mit gleichen Sicherheitseinstellungen zu einem „*Typ*" zusammengefaßt. Das ist sehr sinnvoll, weil oft viele oder sogar alle Dateien eines Verzeichnisses die gleichen Sicherheitseinstellungen haben. Damit kann man oft mit einem Blick die Sicherheitseinstellungen eines ganzen Verzeichnisses erfassen. Bei Auswahl eines *Typs* werden im Inhaltsfenster alle Verzeichnisse bzw. Dateien markiert, die die Sicherheitseinstellungen dieses *Typs* haben. Im Sicherheitsinformationsfenster werden gleichzeitig die Details angezeigt.
+ Außerdem kann ein *Typ* eingefärbt werden. Alle Verzeichnisse bzw. Dateien mit den gleichen Sicherheitseinstellungen werden dann mit der gleichen Farbe dargestellt. (siehe Farbe auswählen)

Abbildung 54: Auszug aus der HILFE-Datei

7.5 VISUAL NETINFO PREVIEW 3

E-mail: fs@informatik.tu-cottbus.de
Homepage: http://www-rnks.informatik.tu-cottbus.de/~fsch/deutsch/index.htm

Beschreibung des Programmierers

Visual NetInfo ist ein NT Netzwerk-Diagnostikwerkzeug, das verschiedenste Informationen über alle Computer in der Domäne sammelt und anzeigt. Visual Netview ist ein sehr nützliches Werkzeug für Netzwerk-Manager, erfahrene Benutzer und Softwareentwickler. Achtung: Dies ist eine Preview Version! Visual Netinfo wurde auf NT 3.51 und NT 4.0 getestet.

Die standardmäßige Aufgabe von Visual Netview ist, folgendes anzuzeigen:

- Alle Rechner in der Domäne
- Geräte
- Dienste
- Laufwerke
- Lokale Gruppen
- Globale Gruppen
- Paßworteinstellungen
- Diverse Informationen über Benutzer
- Netzwerk-Statistiken
- Freigaben

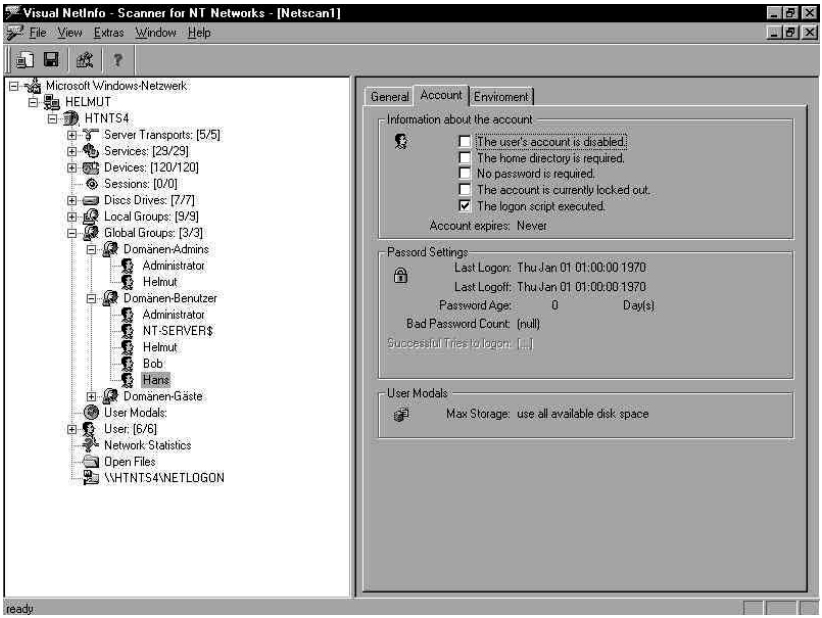


Abbildung 55: Visual Netinfo

7.6 SECURITY CONFIGURATION WIZARD NT 1.5

E-mail: fs@informatik.tu-cottbus.de

Home page: http://www-rnks.informatik.tu-cottbus.de/~fsch/deutsch/ index.htm

Beschreibung des Programmierers

Security Config Wizard NT ist ein Werkzeug zum Setzen einer Vielzahl verschiedener sicherheitsrelevanter Parameter einer Windows NT-Installation. Es ist möglich, diese Einstellungen über alle erreichbaren Domänen hinweg auf den entsprechenden Rechnern zu tätigen, wenn die entsprechenden Zugriffsrechte vorhanden sind. Security Config Wizard NT ist ein nützliches Werkzeug für Netzwerkmanager, Power User und Softwareentwickler.

Security Config Wizard NT ist *nicht* schon wieder ein TweakUI oder WinHacker oder sonst was, sondern beschränkt sich nur auf spezielle sicherheitsrelevante Einstellungen von Windows NT, die zudem schlecht oder teilweise gar nicht dokumentiert sind! Schließlich soll das Rad nicht zum zweiten Male erfunden werden (d. h. allerdings auch, daß wir nichts GEGEN diese Programme haben – wir nutzen sie auch selber)!

Achtung: Viele Änderungen werden in der Registrierdatenbank von Windows NT getätigt. Es sollte vorher eine Sicherheitskopie der Registry erstellt werden, denn Manipulationen an der Registrierung kann einer NT-Maschine erheblichen Schaden zufügen!

Security Config Wizard NT kann:

- Anzeigen und Manipulieren diverser Systeminformationen wie normale Einstellungen über NT
- Sicherheitsrelevante Einstellungen
- Einstellungen des Logon-Prozesses und Logon-Sicherheit
- Sicherheitseinstellungen
- Audit-Einstellungen (Protokollierung von NT)
- Crashcontrol-Einstellungen / Communication Einstellungen / Dateisystem-Einstellungen
- Einige verschiedene Einstellungen wie Performance-Verbesserungen oder Usability-Verbesserungen

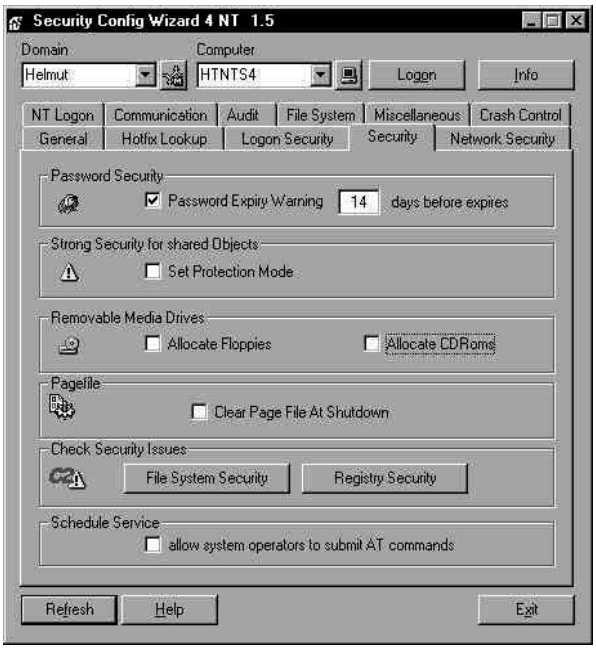


Abbildung 56: Security Configuration Wizard

8 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, daß vieles, was bei der Begehung geprüft wurde, untergeht, weil es vergessen wurde. Dies liegt oft daran, daß keine genügende Vorbereitung stattfand und/oder daß 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.

8.1 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 z. B. 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 Einsetzvorgang abzuspeichern. Am Ende der Begehung liegt 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.

8.2 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 Domänenadministrator 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 an-schließend 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 (siehe z. B.: Abschnitt 7.). 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.

8.3 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.

8.4 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 komplett NTFS-formatiert? Welches zusätzliche Betriebssystem?

8.5 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

8.6 RICHTLINIEN

18. Welche Einstellungen haben die Kontenrichtlinien 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	Gruppen-zugehörigkeit

8.7 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

8.8 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 personenbezogenen 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 ☐

8.9 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 ☐

8.10 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 –	☐
6 34	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?

8.11 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?

8.12 INSTALLIERTE SOFTWARE/ZUSATZSOFTWARE

Die folgenden Fragen sollen dazu dienen, zu erfahren, ob neben den Standardwerkzeugen eigene eingebracht wurden, um das System sicherer zu machen.

50. Wird in den Windows NT-Systemen zusätzlich Software eingesetzt, die der Überwachung des Systems dient? Wenn ja, auf welchem Rechner welche Software?

---

51. Werden für die Verwaltung von Benutzern zusätzliche Werkzeuge eingesetzt? Wenn ja, welche?

8.13 HINWEISE ZUR CHECKLISTE

In diesem Abschnitt werden Hilfestellungen zur Bewertung der Begehungsergebnisse gegeben.

1. Auskunft über die Domäne, an der der verwendete Rechner sich anmeldet, gibt das NETZWERK in START ➡ EINSTELLUNGEN ➡ SYSTEMSTEUERUNG.
2. Auskunft über die Klasse des Rechners gibt der Befehl »net accounts« in der Eingabeaufforderung. Wenn der Befehl erfolgreich abgearbeitet wurde, ist in der Zeile »Rolle des Computers« ersichtlich, als was der Rechner konfiguriert ist. Ist der Rechner ein einfacher Arbeitsgruppenserver, so ist die Ausgabe nur SERVER. Handelt es sich bei dem Windows NT-System um einen Primären Domänen-Controller (PDC), wird PRIMARY ausgegeben.
3. Da es sich bei der Begehung um einen Administratorenarbeitsplatz handeln muß (sonst ist das ganze wenig ergiebig), steht der SERVERMANAGER unter START ➡ PROGRAMME ➡ VERWALTUNG (allgemein) zur Verfügung. Er zeigt alle am PDC »registrierten« Rechner und ihren Typ (PDC, BDC, Server oder Workstation) an.
4. Die Frage nach weiteren Domänen kann nur insoweit vom System beantwortet werden, als sich diese Domänen vertrauen (siehe Frage 5). Weitere Domänen können nur mündlich abgefragt werden.

5./6. Informationen zu Vertrauensstellungen zwischen Domänen erhält man aus dem Benutzermanager. Dieser ist unter START ➡ PROGRAMME ➡ VERWALTUNG (ALLGEMEIN) ➡ BENUTZERMANAGER für DOMÄNEN ➡ RICHTLINIEN-VERTRAUENSSTELLUNGEN zu finden. Ist in mindestens einem Feld ein anderer Rechner eingetragen, so gibt es Vertrauensstellungen in der untersuchten Domäne.

7. Der Befehl net config server zeigt unter »Unsichtbarer Server« die Sichtbarkeit des aktuellen Rechners im Netz an. Alternativ ist die Information in der Registry unter HKEY_LOCAL_MACHINE \System\Services\LanmanServer\Parameters zu erfahren. Ist dort ein Wert HIDDEN und der Text 1 eingetragen, ist der abgefragte Rechner versteckt. Achtung, andere versteckte Rechner können nicht über den beschriebenen Weg abgefragt werden (es sei denn, der Name ist bekannt), darüber muß außerhalb des Systems Auskunft gegeben werden.
8. Diese Information liefert eines der NT-Administrationswerkzeuge: START ➡ Programme ➡ Verwaltung (allgemein) ➡ Festplattenmanager. In der Anzeige werden Laufwerksbuchstaben, Formatierung angezeigt. Das Klicken auf ein Laufwerk zeigt dessen Eigenschaften an.

9.- 11. Die Mitglieder der Gruppe Domänen-Administrator und Administrator sind aus: START ➡ PRROGRAMME ➡ VERWALTUNG (allgemein) ➡ <Klicken auf die jeweilige Gruppe> zu erfahren. DumpACL druckt eine sortierte Liste der Gruppen und ihrer Mitglieder.

12. Prinzipiell gilt, daß sich in einer Domäne der Administrator immer auf *alle* Rechner aufschalten kann, soweit seine Mitgliedschaft in der lokalen Administratorgruppe der Einzelrechner nicht entfernt wurdet. START ➡ PROGRAMME ➡ VERWALTUNG (allgemein) ➡ BENUTZERMANAGER für DOMÄNEN.

13. Das System kann diese Frage nicht beantworten, aber der Arbeitgeber kann es der Interessenvertretung schriftlich mitteilen. Sofern es ein verbindliches Freigabeverfahren für die Benutzerverwaltung gibt, müßte diese Information dort zur Verfügung stehen.

14. Für eine Anzeige aller Gruppen, seien es lokale oder globale Gruppen, kann der BENUTZERMANAGER benutzt werden. Möchte man auf einfache Art und Weise lokale und globale Gruppen getrennt aufgelistet haben, sind die Kommandozeilenbefehle »net group« und »net localgroup« zu empfehlen. Werden beide Befehle ohne Parameter aufgerufen, zeigen sie beide die verschiedenen eingerichteten Gruppen an. Das Kommando »net group« zeigt alle globalen Gruppen an. Für die Anzeige aller lokalen Gruppen ist der Befehl »net localgroup« zu benutzen.

15. Sofern existent, müßte hier die Dokumentation des »Freigabeverfahrens Benutzerkonten« herangezogen werden.

16. Der RAS-SERVER unter START ➡ PROGRAMME ➡ VERWALTUNG (allgemein) gibt unter dem Menüpunkt Remote-Zugriffsberechtigungen genau an, wer welche RAS-Berechtigungen hat.

17. Die Information steht in START ➡ PROGRAMME ➡ VERWALTUNG (allgemein) ➡ BENUTZERMANAGER für DOMÄNEN ➡ <Klick auf jeden Benutzer und dann »Zeiten« bzw. »Anmelden an« auswählen>. Programme wie DumpACL geben diese Information über den gesamten ausgewählten Rechner aus.

18. Die Information steht in START ➡ PROGRAMME ➡ VERWALTUNG (allgemein) ➡ BENUTZERMANAGER für DOMÄNEN ➡ KONTEN. Durch gleichzeitiges Drücken der Tasten STRG+Druck wird das aktuelle Bild in die Zwischenablage des Rechners gespeichert und kann von dort zur Dokumentation in z. B. eine Word-Datei eingesetzt werden.

19. Falls die Interessenvertretung die Namen anderer sie interessierender Rechner kennt, können diese direkt im Benutzermanager ausgewählt werden und die Information abgefragt werden. Falls Namen unbekannt sind, sollte der Arbeit-

geber aufgefordert werden, eine verbindliche Erklärung zu allen Rechnern abzugeben oder für die abweichenden Rechner Bilddrucke (wie vorher geschildert) anzufertigen. Links oben in der Ecke wird der Domänenname bzw. der Rechnername ausgegeben.

20./21. Mit DumpACL lassen sich die Benutzerrechte jedes einzelnen Rechners vollständig anzeigen und in der Vollversion auch ausdrucken.

22./23. Siehe 18./19.

24. Systemrichtlinien für Domänen werden auf dem PDC unter %system root%/system32/ repl/ Import/ Scripts als Datei NTCONFIG.POL gespeichert. Windows 95-Richtlinien werden als CONFIG.POL gespeichert. Systemrichtlinen lassen sich nur im Richtlinieneditor anzeigen!
Sie können natürlich auch als Bilddruck in die Zwischenablage kopiert und in einer Textdatei abgespeichert werden.

25. Vorlagedateien für Richtlinien werden im Verzeichnis %system root%/system32/inf als Datei mit der Endung ADM abgespeichert, z. B. WINNT.ADM oder FORBA.ADM. Diese Dateien sind reine Textdateien und können ausgedruckt werden.

26. Zum Thema der Benutzerprofile siehe Abschnitt 3.4.

27. Diese Informationen sind nicht aus dem System zu erfahren. Hierzu muß die Administration Auskunft geben können. Falls es bereits explizite Datenverzeichnisse oder andere als schützenswert bezeichnete Verzeichnisse/Dateien gibt, können diese natürlich immer »per Hand« untersucht werden: Objekt markieren ➡ EIGENSCHAFTEN ➡ SICHERHEIT ➡ ÜBERWACHUNG.

28. Die beiden Editoren REGEDIT.EXE und REGEDT32.EXE werden üblicherweise in %system root%\system32 gespeichert. Falls sie dort nicht zu finden sind, hilft START ➡ SUCHEN ➡ <reg*.exe>.

29./30. Siehe 2.

31./32. Die Übersicht des Datenschutzbeauftragten gemäß § 37 Abs. 2 BDSG müßte dazu Auskunft geben.

33. Die Besitzer von Dateien sind mit Windows NT-eigenen Mitteln nur per Hand für jede Datei abfragbar. Der Sicherheitsmanager (siehe Abschnitt 7.4) zeigt Besitzer, Berechtigte und ihre Rechte in der Darstellungsweise des Windows NT-Explorers an.

34.-36. Siehe 27.

37. Freigaben sind für den jeweiligen Rechner am Symbol der ausgestreckten Hand erkennbar. Mit dem Kommandozeilenbefehl NET SHARE werden alle Freigaben des Rechners angezeigt.

38. Die Freigaberechte sind mit Windows NT-eigenen Mitteln nur per Hand für jede Datei abfragbar. Der Sicherheitsmanager (siehe Abschnitt 7.4) gibt einen schnelleren Überblick.
39. Administrator und Datenschutzbeauftragten fragen.
40. Siehe 39.
41. Die Aufstellung der RAS-Berechtigten ist im RAS-Manager (Abschnitt 2.9) abzufragen. DumpACL (Abschnitt 7.2) erzeugt eine Benutzerliste mit differenzierten RAS-Angaben.
42. Administrator und Datenschutzbeauftragten fragen.
43. Administrator fragen. Die Protokolle können als Textdateien, aber auch im Format der Ereignisanzeige gespeichert werden.
44. Verzeichnis anklicken. Rechte Maustaste ➡ Eigenschaften ➡ Sicherheit ➡ Überwachung.
45. Administrator und Geschäftsleitung fragen.
46. Rechte anlegen, löschen oder ändern sollte in einer geregelten Verfahrensweise festgelegt werden. Administrator und Geschäftsleitung fragen.

47.–51 Administrator und Geschäftsleitung fragen.

9 BEISPIEL FÜR EINE WINDOWS NT-VEREINBARUNG

Die nachfolgende Vereinbarung ist keine Mustervereinbarung im Sinne einer Blaupause, denn betriebliche NT-Installationen sind nur im Ausnahmefall Kopien anderer EDV-Installationen. Wir halten es eher für schädlich als hilfreich, wenn Vereinbarungen anderer Betriebe »einfach« übernommen werden. Besonders bei komplizierten DV-Systemen ist es nach unserer Meinung wichtig, wenn nicht sogar unverzichtbar, daß die Interessenvertretung jeden Punkt ihres Entwurfes kennt und auf Nachfragen des Arbeitgebers auch erläutern und begründen kann. Um dies zu gewährleisten, muß sich die Interessenvertretung mit jedem Satz befassen, ihn diskutieren, gegebenenfalls verändern und erst dann in den eigenen Text aufnehmen.

Jede Vereinbarung ist das Ergebnis eines mehr oder minder langen Verhandlungsprozesses. Das betriebliche und persönliche Klima zwischen den handelnden Personen bestimmt fast immer den Detaillierungsgrad von Vereinbarungen. Auch vor diesem Hintergrund sollten zu einem Regelungsthema am besten mehrere Vereinbarungen/Entwürfe anderer Betriebe zur Information herangezogen werden. Diese sollten dann aber immer als Beispiele für bestimmte – dem Leser meist unbekannte – betriebliche Situationen gesehen werden und nicht als Kopiervorlage für das eigene Handeln angesehen werden. Das folgende Vereinbarungsbeispiel ist dementsprechend eine Zusammenstellung aus verschiedenen Diskussionen, Entwürfen und Vereinbarungen. Es enthält solche Themen, von denen wir denken, daß sie in einer Vereinbarung geregelt werden sollten.

BETRIEBSVEREINBARUNG
ZWISCHEN

MÜLLER GMBH (NACHFOLGEND ARBEITGEBER)
UND

BETRIEBSRAT DER MÜLLER GMBH (NACHFOLGEND BR)
ZUR EINFÜHRUNG, ANWENDUNG UND ÄNDERUNG / ERWEITERUNG VON WINDOWS NT

1. GEGENSTAND

Diese Betriebsvereinbarung regelt

1. die Einführung, Anwendung und Änderung/Erweiterung des Betriebssystems Microsoft Windows NT,
2. die Verarbeitung und/oder Nutzung von personenbezogenen Daten der Arbeitnehmerinnen und Arbeitnehmer mit dem Betriebssystem Microsoft Windows NT.

Soweit diese Vereinbarung nichts anderes regelt, gelten die Bestimmungen der Rahmenvereinbarung EDV vom 1.5.1993.

2. GELTUNGSBEREICH

Die Betriebsvereinbarung gilt für alle Arbeitnehmerinnen und Arbeitnehmer des Arbeitgebers. Ausgenommen von den Schutzregelungen dieser Vereinbarung sind leitende Angestellte entsprechend § 5 Abs. 2 BetrVG.

Die Betriebsvereinbarung gilt für alle Betriebsstätten des Arbeitgebers.

3. BEGRIFFSBESTIMMUNGEN

Rechner im Sinne dieser Vereinbarung sind Server, Arbeitsplatzrechner, Laptops und sonstige technische Einrichtungen, auf denen das Betriebssystem Windows NT installiert ist.

NT-Rechner bzw. NT im Sinne dieser Vereinbarung steht für jedes beim Arbeitgeber installierte Windows NT-Betriebssystem, unabhängig von der Typart.

Typarten im Sinne dieser Vereinbarung sind Windows NT-Server und Windows NT-Workstation, wobei die unterschiedlichen Funktionalitäten des Servers als PDC, BDC oder Server unberücksichtigt bleibt.

4. GRUNDSÄTZLICHES

4.1 Verarbeitung personenbezogener Daten

Die Verarbeitung oder Nutzung von Daten der Arbeitnehmerinnen und Arbeitnehmer mit Windows NT ist ausschließlich entsprechend den in dieser Betriebsvereinbarung vereinbarten Zwecken zulässig, d. h., die vereinbarten Zwecke sind in den Anlagen zu dieser Vereinbarung abschließend dokumentiert. Sind Zwecke in den Anlagen nicht konkret benannt, gelten sie als nicht vereinbart und sind unzulässig. Die Beweislast für die Zulässigkeit der Verarbeitung von Daten der Arbeitnehmerinnen und Arbeitnehmer mit NT trägt der Arbeitgeber.

4.2 Domänenkonzept

Der Arbeitgeber führt ein Domänenkonzept ein. Mit diesem werden die eingesetzten NT-Rechner verwaltet sowie Benutzerverwaltung und Zugriffsverwaltung auf Dateien, Drucker und anderen Netzwerkressourcen durchgeführt. Die lokalen Ressourcen werden auf den einzelnen Arbeitsplatzrechnern durch den Benutzer verwaltet.

Benutzer werden nur auf PDCs angelegt, d. h., es gibt keine lokalen Benutzerkonten. Ausgenommen sind die nicht zu löschenden Benutzerkonten Administrator und Gast sowie das Konto Hauptbenutzer (PowerUser). Zusammengehörende globale Gruppen und lokale Gruppen erhalten auf allen NT-Rechnern der Domäne – soweit technisch nicht unmöglich – identische Namen.

4.3 ADMINISTRATION

Die Administration der Domäne erfolgt derzeit durch Mitarbeiter des jeweiligen Standorts. Soweit organisatorisch möglich, sollen die Konten »Domänen-Administrator« in der Domäne und »Administrator« auf dem lokalen NT-Rechner nicht genutzt werden. Statt dessen sollen die vordefinierten Sub-Administratorkonten Server-Operator, Konten-Operator, Sicherungs-Operator und Drucker-Operator für Administrationsaufgaben verwendet werden.

Jeder Sub-/Administrator erhält zusätzlich ein Benutzerkonto ohne Sub-/Administrationsrechte. Die Nutzung aller Administratorkonten ist ausschließlich administrativen Tätigkeiten vorbehalten.

Der Administrator ist nicht berechtigt, ohne vorherige Zustimmung des jeweiligen Anwenders die Funktion »Besitz übernehmen« auszulösen. Sollte die vorherige Zustimmung des Anwenders nicht einholbar sein (z. B. bei Krankheit), kann diese auch durch die Zustimmung des jeweils zuständigen Betriebsrates ersetzt werden.

4.4 BENUTZER AM ARBEITSPLATZRECHNER

Benutzer eines Arbeitsplatzrechners können zusätzlich zum Eintrag als Domänen-Benutzer als lokaler Hauptbenutzer eingetragen werden. In diesem Fall können sie Freigaben und Zugriffsberechtigungen erteilen, bei denen die Regelungen dieser Vereinbarung verbindliche Vorgabe sind. Ist kein Hauptbenutzerkonto eingerichtet, erfolgen Freigaben und Zugriffsberechtigungen durch die Domänen-Administratoren.

Für jeden Benutzer eines Arbeitsplatzrechners wird ein Verzeichnis, auf das ausschließlich dieser Benutzer Zugriff hat, eingerichtet. Alle Benutzer haben das Recht, Dateien durch Verschlüsselung zu schützen. Die Verwendung von Verschlüsselungsprogrammen bedarf der Abstimmung mit DV/Benutzerservice und der Zustimmung des Betriebsrates, soweit es sich nicht um private Dateien handelt.

Die Benutzer erhalten die Möglichkeit, mit der Ereignisanzeige den Zugriff zu den vor ihnen genutzten Dateien und Ordnern zu prüfen.

4.5 GRUPPEN- UND BENUTZERPROFILE

Der Benutzergruppe JEDER werden die Zugriffsrechte, soweit dies technisch möglich und sinnvoll ist, entzogen. Das Konto GAST wird deaktiviert.

Integrierte Benutzerberechtigungen, Rechte über Freigaben und Zugriffsrechte für Gruppen und Benutzer sind restriktiv zu vergeben. Für die Vergabe von Benutzerberechtigungen, Freigaben und Zugriffsrechten wird innerhalb von drei Monaten nach Abschluß dieser Vereinbarung ein formales Freigabeverfahren entwickelt und mit dem Betriebsrat in einem Zusatz zu dieser Vereinbarung verbindlich festgelegt.

Bei der erstmaligen Einrichtung erhält jeder Benutzer vom Kontenadministrator ein einmaliges Paßwort, das bei der ersten Anmeldung geändert werden muß. Die Sperrung von Paßwörtern gegen Änderung durch den Benutzer ist unzulässig.

4.6 GRUPPE REVISION

Auf Domänenebene (globale Gruppe) und auf jedem NT-Rechner (lokale Gruppe) wird eine Gruppe REVISION angelegt. Diese Gruppen erhalten als einzige Gruppe auf ihrem Rechner die Benutzerberechtigung »Verwalten von Überwachungs- und Sicherheitsprotokoll«. Nur die globale Gruppe REVISION wird Mitglied der lokalen REVISION.

Mitglieder der Gruppe REVISION sind die Mitglieder des EDV-Ausschusses des Betriebsrats und der betriebliche Datenschutzbeauftragte. Administratoren dürfen nicht Mitglied einer Gruppe REVISION sein. Die Gruppe REVISION erhält für alle Verzeichnisse Leserecht. Ausgenommen davon sind alle für die Verwaltung und Organisation der Ereignisprotokolle verwendeten Verzeichnisse, auf denen die Gruppe das Recht VOLLZUGRIFF erhält.

4.7 SYSTEMRICHTLINIEN UND BENUTZERPROFILE

Soweit Systemrichtlinien und/oder Benutzerprofile eingesetzt werden sollen, wird der Betriebsrat informiert und gegebenenfalls seine Zustimmung eingeholt.

4.8 FERNZUGRIFF (RAS)

In begründeten Ausnahmefällen werden unter Beachtung der geltenden Arbeitszeitregelungen gesonderte Benutzerkonten für den RAS-Zugang eingerichtet. Diese Konten erhalten das Recht KEIN ZUGRIFF auf das Verzeichnis DATEN.

4.9 EXTERNE BENUTZER

Soweit der Arbeitgeber fremden Mitarbeitern eigene Benutzerrechte in der Domäne, auf einem Server oder einer Workstation einräumt, dürfen diese Benutzer keine Administrationsrechte, keine besonderen Benutzerberechtigungen und keinen RAS-Zugriff erhalten.

Fremde Benutzer sind in eigenen Gruppen zu organisieren, d. h. sie dürfen nicht in betriebsinternen globalen oder lokalen Gruppen Mitglied werden. Die Benutzerkonten sind zeitlich auf drei Monate zu befristen.

4.10 SICHERHEIT, ZUGRIFF UND ÜBERWACHUNG

Jeder NT-Rechner läuft ausschließlich unter NTFS. Die Einrichtung von anderen Betriebssystemen ist unzulässig.

Dateien mit personenbezogenen Daten sind grundsätzlich in einem einzigen Verzeichnis (z. B. DATEN) auf einem Server abzulegen. Die Speicherung derartiger Daten in anderen Verzeichnissen des Servers oder auf einer lokalen Festplatte ist unzulässig.

Die Gruppen NETZWERK, JEDER sowie alle Gruppen/Benutzer mit RAS-Zugang erhalten das Zugriffsrecht KEIN ZUGRIFF auf das Verzeichnis DATEN und alle Unterverzeichnisse und Dateien.

Auf jedem NT-Rechner ist die Verzeichnisüberwachung für das Datenverzeichnis sowie alle Unterverzeichnisse und die Dateiüberwachung für alle Dateien grundsätzlich zu aktivieren. Der konkrete Umfang der Aktivierung wird zwischen Betriebsrat und Geschäftsleitung innerhalb von drei Monaten nach Abschluß dieser Vereinbarung in einem Zusatz zu dieser Vereinbarung verbindlich festgelegt.

4.11 EREIGNISPROTOKOLLE

4.11.1 Überwachungsrichtlinien

Die Überwachungsfunktion wird auf jedem NT-Rechner mit Ausnahme der Prozeßüberwachung aktiviert.

Die Einstellungen für die drei Ereignisprotokollarten betragen jeweils 2048 KB und »Ereignisse überschreiben falls nötig«. Alle Protokolle werden vor der Löschung durch die REVISION archiviert. Das Archivverzeichnis muß im Verzeichnis DATEN liegen. Eigentümer und alleiniges Zugriffsrecht soll die Gruppe REVISION haben.

Die Einsichtnahme und Nutzung der Ereignisprotokolle und der archivierten Protokolle erfolgt über das Programm »Ereignisanzeige« und ist den Administratoren zur Behebung technischer Probleme gestattet. Die Weitergabe von Daten aus Ereignisprotokollen an Personen außerhalb der Administrationsgruppe bedarf der Zustimmung durch den Betriebsrat.

4.11.2 Sicherheitsprotokoll

Im Sicherheitsprotokoll (Security Log – Datei SecEvent.evt im Verzeichnis WINNT\system32\config) eines NT-Rechners werden alle Zugriffe zur Domäne (auf dem PDC bzw. den BDCs) bzw. zu den lokalen NT-Rechnern protokolliert.

4.11.3 Systemprotokoll

Im Systemprotokoll (System Log – Datei SysEvent.evt im Verzeichnis WINNT\system32\config) werden Systemereignisse protokolliert.

4.11.4 Anwendungsprotokoll

Im Anwendungsprotokoll (Application Log – Datei AppEvent.evt im Verzeichnis WINNT\system32\config) werden von Anwendungsprogrammen ausgelöste Ereignisse protokolliert.

5. DATENSCHUTZ UND VERSCHLÜSSELUNG

Der Arbeitgeber wird ein auf Windows NT spezifiziertes Datenschutz- und Sicherheitskonzept erarbeiten. Das Konzept beinhaltet auch Verfahrensweisen für die Verschlüsselung. Das Konzept ist dem Betriebsrat innerhalb von drei Monaten nach Abschluß dieser Vereinbarung vorzulegen, seine Zustimmung ist einzuholen.

6. QUALIFIZIERUNGSMASSNAHMEN

Allen Arbeitnehmerinnen und Arbeitnehmer, die an NT-Rechnern arbeiten bzw. zukünftig arbeiten sollen, wird eine Schulung über die Benutzung von Windows NT angeboten. Die Schulung findet während der Arbeitszeit statt. In der Schulung werden neben fachlichen Kenntnissen zu Windows NT und dessen Anwendung auch der Inhalt dieser Betriebsvereinbarung vermittelt. Das Schulungskonzept ergibt sich aus der Anlage XX. Die Teilnahme an der Schulung ist mit Zertifikat zu bestätigen. Bei der Auswahl der Dozenten ist § 98 BetrVG zu beachten.

7. DOKUMENTATION

Die folgenden Dokumentationen geben den Stand der NT-Installation zum Zeitpunkt des Abschlusses dieser Vereinbarung wieder. Sofern Veränderungen der Inhalte der Anlagen geplant sind, wird entsprechend Ziffer 8 verfahren.

Die Dokumentation erfolgt – soweit technisch möglich – mit den NT-Verwaltungsprogrammen bzw. den zur Verfügung stehenden Hilfsprogrammen zur Bearbeitung von Bildschirmfotos.

7.1 DOMÄNEN

Das Domänenkonzept wird in Anlage 0 dokumentiert.

7.2 HARDWARE

Zum Abschluß dieser Vereinbarung eingesetzte

- Domänen-Controller werden in Anlage 1 dokumentiert,
- Backup-Domänen-Controller werden in Anlage 2 dokumentiert,
- Server werden in Anlage 3 dokumentiert,
- NT Workstations werden in Anlage 4 dokumentiert,
- sonstige Rechner in den Domänen sind in Anlage 5 dokumentiert.

Die Dokumentationen enthalten, gegliedert nach Bereichen und Abteilungen, die Rechnerbezeichnung, die IP-Nummer, die Inventarnummer, den Standort (Verweis zur Anlagendokumentation in DV/Benutzerservice) .

7.3 SOFTWARE

Zum Zeitpunkt des Abschlusses dieser Vereinbarung werden folgende Betriebssysteme eingesetzt: Microsoft Windows NT Server (PDC, BDC und Server) in den Versionen 3.51 und 4.0 und Microsoft Windows NT Workstation in der Version 4.0.

7.4 BENUTZER- UND GRUPPENPROFILE

Zum Abschluß dieser Vereinbarung definierte

- Globale Gruppen werden in Anlage 5 dokumentiert,
- Lokale Gruppen werden in Anlage 6 dokumentiert,
- Administratoren werden in Anlage 7 dokumentiert,
- Benutzer werden in Anlage 8 dokumentiert.

Die Dokumentationen enthalten, gegliedert nach Domäne und NT-Rechner, den Namen der Gruppe, Art der Gruppe und die Benutzernamen der Gruppe sowie Benutzernamen ohne Gruppenzugehörigkeit.

Bei DV/Benutzerservice wird eine detaillierte Dokumentation aller Domänen und der auf ihnen eingerichteten Gruppen und Benutzer mit allen ihren zugewiesenen Rechten geführt.

7.5 INTEGRIERTE BENUTZERRECHTE

In Anlage 9 werden alle Benutzer- oder Gruppenkonten mit den ihnen zugewiesenen integrierten Benutzerrechte dokumentiert.

7.6 KONTENRICHTLINIEN

In Anlage 10 werden die Einstellungen der Kontenrichtlinien des PDC dokumentiert.

7.7 ÜBERWACHUNG

In Anlage 11 werden die Einstellungen aller überwachten Verzeichnisse und Dateien dokumentiert.

7.8 WEITERE NT-ANWENDUNGEN UND HILFSPROGRAMME

Alle zum Zeitpunkt des Inkrafttretens dieser Vereinbarung von Microsoft mit dem Betriebssystem NT ausgelieferten Verwaltungsprogramme sind in Anlage 12 mit Angabe von Programmname, Dateiname, Version, Kurzbeschreibung, Speicherort, zugriffsberechtigte Benutzer dokumentiert.

Soweit zusätzliche Programme zur Verwaltung und Organisation von Windows NT angewendet werden, sind diese in Anlage 13 mit Angabe von Programmname, Dateiname, Version, Kurzbeschreibung, Speicherort, zugriffsberechtigte Benutzer dokumentiert.

8. ÄNDERUNGEN UND ERWEITERUNGEN

Bei allen Änderungen (neue Versionen) und Erweiterungen (Servicepacks, HotFixes, Patches) wird entsprechend der Rahmenvereinbarung EDV verfahren, d. h., vor einer

Zustimmung des Betriebsrates dürfen keine Änderungen und/oder Erweiterungen auf produktiven Rechnern umgesetzt werden.

9. MEINUNGSVERSCHIEDENHEITEN

Bei Meinungsverschiedenheiten über die Anwendung dieser Vereinbarung sowie in den Fällen, in denen die Zustimmung des Betriebsrates nach dieser Vereinbarung notwendig ist, aber nicht erteilt wurde, entscheidet die Einigungsstelle gemäß § 76 Abs. 5 BetrVG. Die Einigungsstelle wird von ..... geleitet. Im Falle der Verhinderung bestimmt sie eine/n Vorsitzende/n. Jede Seite ist mit drei Beisitzern vertreten. Die Einigungsstelle tritt auf Anrufung einer Seite innerhalb von 14 Tagen zusammen.

10. SCHLUSSBESTIMMUNGEN

Diese Vereinbarung tritt mit Abzeichnung der Anlagen durch beide Parteien in Kraft.

Sie kann mit einer Frist von einem Monat zum Quartalsende, erstmals zum ..... gekündigt werden.

Für den Fall der Kündigung ist die Nachwirkung vereinbart.

Die Anlagen 0 bis 13 sind Bestandteil der Betriebsvereinbarung.

10.1 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

Kuppinger, Martin; Windows 2000 – Die Neuerungen im Überblick, Microsoft Press 1999

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

10.2 LITERATUR (ENGLISCH)

Espinola, Michael ; The Hardening of Microsoft Windows NT V4, Rev 1, Bezug über http://pweb.netcom.com/~honeyluv/hardennt.html

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

Murray, James D.; Windows NT Event Logging; O´Reilly 1998

Sheldon, Tom; Windows NT Security Handbook, McGraw-Hill 1997

Windows NT Magazine: www.winntmag.com. Sehr gutes Magazin, alle (!) Hefte werden komplett mit dreimonatiger »Verzögerung« im Internet veröffentlicht (inklusive Suchmaschine)

10.3 INTERNET RESSOURCEN (DEUTSCH)

Windows NT – Einführung und Konzepte von Georg Lucas und Bernhard Tritsch http://www.igd.fhg.de/www/grz/mswin/index.html#Seminar

International Network of Institutions for Computer Graphics, Windows NT Development and Solution Center: http://www.igd.fhg.de/www/grz/devnsol/index.html

10.4 INTERNET RESSOURCEN (ENGLISCH)

Wahrscheinlich die beste FAQ zu Windows NT: John Savill's www.ntfaq.com

Verschiedene excellente Tools: www.sysinternals.com/util.htm

Trusted Systems: www.trustedsystems.com

Sicherheitstools: www.somar.com

10.5 ELECTRONIC NEWSLETTERS (DEUTSCH)

Windows NT Newsletter (PC Magazin): www.wekanet.de/news

10.6 ELECTRONIC NEWSLETTERS (ENGLISCH)

Sunbelt Windows NTools E-News: www.sunbelt-software.com

ESI Tech Support Mail List: www.execsoft.com/tech-support

Windows NT Magazin UPDATE , wöchentlicher newsletter. www.winntmag.com/update

Zweiwöchentlicher Newsletter: http://www.executive.com/eletter

Verschiedene gute Mailinglisten zu NT- und EDV-Sicherheit http://xforce.iss.net/mail-lists

10.7 MICROSOFT-QUELLEN (DEUTSCH)

Server: http://www.eu.microsoft.com/germany/backoffice/ntserver/

Workstation: http://www.eu.microsoft.com/germany/ntworkstation/

Servicepack 5:
http://www.microsoft.com/ntserver/nts/downloads/recommended/sp5/

Downloads: http://www.eu.microsoft.com/germany/download/

D

E

F

G

12 ABBILDUNGSVERZEICHNIS

Hans-Böckler-Stiftung

Die Hans-Böckler-Stiftung des Deutschen Gewerkschaftsbundes (DGB) wirbt für die Mitbestimmung als Gestaltungsprinzip einer demokratischen Gesellschaft. Sie tritt dafür ein, Mitbestimmungsrechte und -möglichkeiten zu erweitern.

Beratung und Schulung

Die Stiftung berät und qualifiziert Betriebs- und Personalräte und Arbeitnehmervertreter in Aufsichtsräten, Männer und Frauen, in wirtschaftlichen und rechtlichen Angelegenheiten, in Fragen des Personal- und Sozialwesens, der beruflichen Aus- und Weiterbildung, der Gestaltung neuer Techniken, des betrieblichen Arbeits- und Umweltschutzes.

Wirtschafts- und Sozialwissenschaftliches Institut (WSI)

Das Wirtschafts- und Sozialwissenschaftliche Institut in der Hans-Böckler-Stiftung forscht zu den Themen »Wirtschaftswandel und Beschäftigung im Globalisierungsprozeß«, »Soziale Polarisierungen, kollektive Sicherung und Individualisierung« und »Arbeitsbeziehungen und Tarifpolitik«.
Das WSI-Tarifarchiv dokumentiert das Tarifgeschehen umfassend und wertet es aus.

Forschungsförderung

Die Abteilung Forschungsförderung der Stiftung vergibt Forschungsaufträge zu den Themen Strukturpolitik, Mitbestimmung, Arbeitsgesellschaft, Öffentlicher Sektor und Sozialstaat.
Die Forschungsergebnisse werden in der Regel nicht nur publiziert, sondern auf Veranstaltungen zur Diskussion gestellt und zur Weiterqualifizierung von Mitbestimmungsakteuren genutzt.

Studienförderung

Ziel der Stiftung ist es, einen Beitrag zur Überwindung sozialer Ungleichheit im Bildungswesen zu leisten. Gewerkschaftlich oder gesellschaftspolitisch engagierte Studierende unterstützt sie mit Stipendien, mit eigenen Bildungsangeboten und der Vermittlung von Praktikantenstellen.
Bevorzugt fördert die Stiftung Absolventinnen und Absolventen des zweiten Bildungsweges.

Öffentlichkeitsarbeit

Ihre Arbeitsergebnisse und Dienstleistungen veröffentlicht die Stiftung über Veranstaltungen, Publikationen, mit PR- und Pressearbeit. Sie gibt zwei Monatszeitschriften heraus: »Die Mitbestimmung« und die »WSI-Mitteilungen«, außerdem die Vierteljahresschrift »South East Europe Review for Labour and Social Affairs (SEER)«, das »Wirtschaftsbulletin Ostdeutschland« und »Network, EDV-Informationen für Betriebs- und Personalräte«.

Hans-Böckler-Stiftung
Abteilung Öffentlichkeitsarbeit
Bertha-von-Suttner-Platz 1
40227 Düsseldorf
Telefax: 0211/7778 - 225
www.boeckler.de

In der edition der Hans-Böckler-Stiftung sind bisher erschienen:

Nr.	Autor/Titel	DM	Bestell-Nr.	ISBN-Nr.
1	*Gertrud Kühnlein* **Neue Typen betrieblicher Weiterbildung**	**18,50**	**13001**	**3-928204-73-4**
2	*Stefan Kühn* **Komplementärer Regionalismus**	**28,00**	**13002**	**3-928204-64-5**
3	*Karl-Hermann Böker, Peter Wedde* **Telearbeit praktisch**	**13,00**	**13003**	**3-928204-75-0**
4	*Peter Ittermann* **Gestaltung betrieblicher Arbeitsorganisation**	**16,00**	**13004**	**3-928204-76-9**
5	*Lothar Kamp* **Gruppenarbeit**	**12,00**	**13005**	**3-928204-77-7**
6	*Hartmut Klein-Schneider* **Flexible Arbeitszeit**	**13,00**	**13006**	**3-928204-78-5**
7	*Siegfried Leittretter* **Betrieblicher Umweltschutz**	**13,00**	**13007**	**3-928204-79-3**
8	*Winfried Heidemann* **Beschäftigungssicherung**	**12,00**	**13008**	**3-928204-80-7**
9	*Wolfhard Kohte* **Die Stärkung der Partizipation der Beschäftigten im betrieblichen Arbeitsschutz**	**18,00**	**13009**	**3-928204-81-5**
10	*Karin Schulze Buschoff* **Teilzeitarbeit im europäischen Vergleich**	**25,00**	**13010**	**3-928204-82-3**
11	*Hans Gerhard Mendius, Stefanie Weimer* **Beschäftigungschance Umwelt**	**28,00**	**13011**	**3-928204-83-1**
12	*Helene Mayerhofer* **Betriebswirtschaftliche Effekte der Fusion von Großunternehmen**	**10,00**	**13012**	**3-928204-85-5**
13	*Winfried Heidemann* **Betriebliche Weiterbildung**	**14,00**	**13013**	**3-928204-86-6**
14	*Hartmut Klein-Schneider* **Leistungs- und erfolgsorientiertes Entgelt**	**16,00**	**13014**	**3-928204-97-4**

Nr.	Autor/Titel	DM	Bestell-Nr.	ISBN-Nr.
15	*Christina Klenner* **Mehr Beschäftigung durch Überstunden-abbau und flexible Arbeitszeitmodelle**	**12,00**	**13015**	**3-928204-88-2**
16	*Annette Henninger* **Ins Netz geholt: Zeit, Geld, Informationen – alles, was die Wissenschaftlerin braucht!?**	**28,00**	**13016**	**3-928204-89-0**
17	*Wolfgang Joußen, Leo Jansen, Manfred Körber* **Informierte Region. Regionale Entwicklungsperspektiven in der Informationsgesellschaft**	**19,00**	**13017**	**3-928204-90-4**
18	*Dietmar Köster* **Gewerkschaftlich ausgerichtete Seniorenbildungsarbeit in der Praxis**	**20,00**	**13018**	**3-928204-91-2**
19	*Michael Kürschner, Helmut Teppich* **Windows NT: Handbuch für Betriebsräte**	**28,00**	**13019**	**3-928204-92-0**
20	*Roland Köstler* **Rechtsleitfaden für Aufsichtsrats-mitglieder nach dem Mitbestimmungs-gesetz '76**	**14,00**	**13020**	**3-928204-84-X**
22	*Lutz Mez, Annette Piening, Klaus Traube* **Was kann Deutschland hinsichtlich eines forcierten Ausbaus der Kraft-Wärme-Kopplung von anderen Ländern lernen?**	**20,00**	**13022**	**3-928204-93-9**

Bestellungen bitte unter Angabe der Bestell-Nr. an:

DER SETZKASTEN GMBH
PRODUKTION · VERLAG · WERBUNG
Am Kreuzberg 4
40489 Düsseldorf
Telefax: 0211 / 408 00 80
E-Mail: lavista@setzkasten.de