Roger Odenthal
Unternehmensberatung

Sicherheit und Prüfung
Von Betriebssystem und Netzwerk
In einer SAP R/3™-Umgebung

Roger Odenthal

Hinweis

Der nachfolgende Leitfaden wurde noch in der Zeit meines alten Prüfungsbüros erstellt und weist dementsprechend noch das hierauf gerichtete Layout auf. Eine inhaltliche Überarbeitung wäre ebenfalls notwendig. Da ich derzeit an weiteren Projekten arbeite ist mir dieses kurzfristig nicht möglich. Ich möchte andererseits Ihre vielen hierauf gerichteten Anfragen nicht zurückweisen und stelle Ihnen das Dokument daher in der vorhandenen Form zur Verfügung.

Ich würde mich freuen, wenn Sie trotz dieser Unzulänglichkeiten Anregungen für Ihre Prüfung finden würden.

Köln, im Juni 2003

Roger Odenthal

Neue Kontaktdaten:

Roger Odenthal Unternehmensberatung
Windmühlenstraße 159-161
51063 Köln
Telefon 0221-4921403
Telefax 0221-4921404
E-Mail: info@roger-odenthal.de
Home: www.roger-odenthal.de

Sicherheit und Prüfung von Betriebssystem und Netzwerk in einer SAP R/3-Umgebung

Roger Odenthal

Inhaltsverzeichnis

Abbildungsverzeichnis

Seite

Fachwörter und Kurzbezeichnungen

ACL	-	Access Control Liste (Datei mit Rechten des einzelnen Anwenders)
Client	-	Arbeitsplatzstation des Anwenders
Container	-	Organisatorische Einheit in einer NDS
Dediziertes-Serverlaufwerk	-	Serverlaufwerke mit genau zugewiesenen Aufgaben
Distributet-Network	-	Verteilung von Client- und Serverfunktion auf (einen) Rechner im Netzwerk
Domänen-Controller	-	Softwarekomponente, die aller Serverlaufwerke eines Netzwerkes als logische EDV-Einheit betrachtet
NDS	-	Novell Directory Services, Softwarekomponente, die eine zentrale Verwaltung aller Objekte eines Netzwerkes ermöglicht
SAM	-	Security-Account-Manager, Zugriffsverwaltung von WINDOWS-NT mit Hilfe einer zugeordneten Datenbank (SAM-Datenbank)
Server	-	Rechner mit Servicefunktion in einem Netzwerk
Skalierung	-	Aufteilung und Erweiterung von Soft- und Hardware

I Installationsumgebung einer SAP R/3-Lösung

1 Modularität und Client-Server-Prinzip

Zentraler Grundgedanke bei SAP ist das Angebot einer Standard-Software-Lösung, die - unabhängig von der Unternehmensgröße - sowohl bei einem kleinen Handwerksbetrieb als auch bei einem großen, multinationalen Konzern ohne wesentliche Änderungen eingesetzt werden kann. Zur Umsetzung dieses Grundgedankens bedarf es - in einer **vertikalen Betrachtung** - der **Modularisierung** in einem Programm implementierter elementarer Softwareprozesse (**Aufgaben**) sowie - in einer **horizontalen Betrachtung** - der beliebigen **Skalierung** dieser Aufgaben (**Prozesse**) auf einer oder mehreren Maschinen.

1.1 Softwaretechnische Betrachtung einer Client-Server-Lösung

Softwaretechnisch betrachtet, wird bereits durch die Technik der "Unterprogrammierung" ein Service zur Verfügung gestellt, auf den andere Programmteile beliebig oft zugreifen können. Eine Weiterentwicklung dieser Technik findet sich mit der objektorientierten Programmierung, die eine weitgehend **Abkapselung und Modularisierung serviceorientierter Programmteile** ermöglicht.

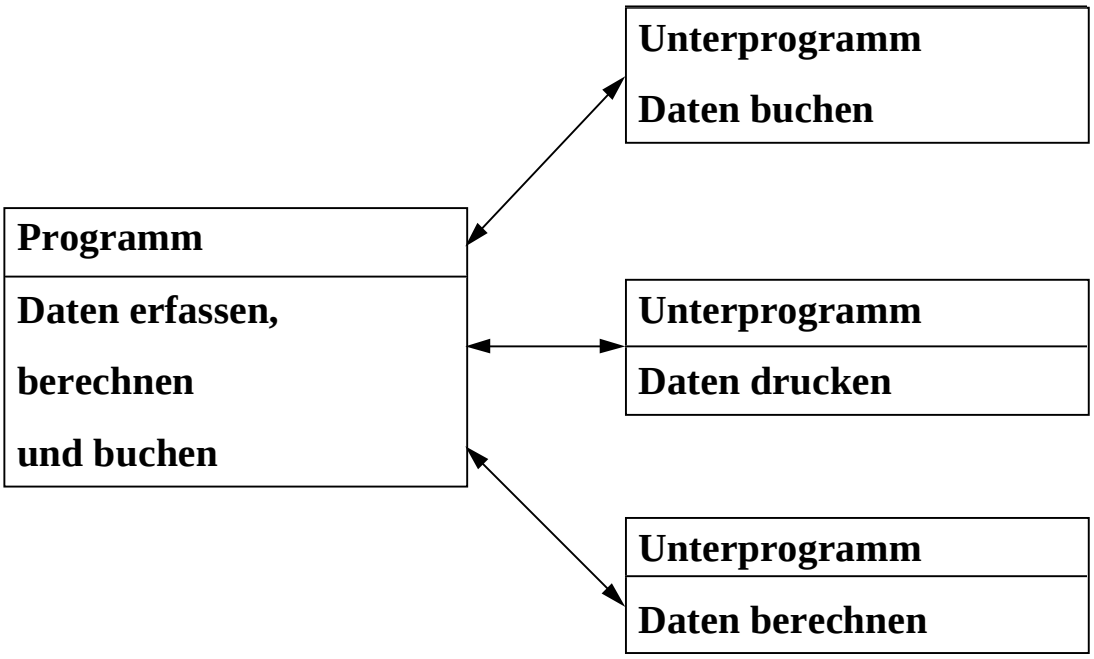

Bild 1 Unterprogramme mit Servicefunktion

1.2 Hardwaretechnische Betrachtung einer Client-Server-Lösung

1.2.1 Alternative Hardwarekonzepte

Eine rein hardwareorientierte Umsetzung des Client-Server-Prinzips finden wir in Netzwerken, bei denen **Rechner mit bestimmten Serviceaufgaben**, wie z.B.

- Druckfunktionalitäten,
- Datenbankhaltung,
- Kommunikation,
- Programmhaltung,

zentral zur Verfügung gestellt werden. Ziele hierfür sind das Teilen teurer Ressourcen, wie z.B. von Druckern, die Vermeidung von Redundanzen bei der Datenhaltung, die Umsetzung von Standards, preiswertere Softwarelizenzen und eine vereinfachte Administration des EDV-Systems.

Die Umsetzung der aufgezeigten Hardwarephilosophie läßt sich mit **alternativen Netzwerkkonzepten** erreichen:

❑ **Verteilte Client-Server-Lösung (Distributed Network)**

Jeder der verbundenen **Rechner übernimmt gleichermaßen Client- und Serverfunktionen** (Workgroup-Prinzip).

Eine entsprechende Lösung kann ggf. in kleinen Netzwerkumgebungen realisiert werden. Gefahren ergeben sich erfahrungsgemäß dadurch, daß eine zentrale Administration und Benutzerverwaltung in einem solch verteilten Netzwerk nicht möglich ist, daß die Nutzeraktivitäten nur sehr schwer einzuschränken sind und sich die verteilten Daten auf allen Rechnern bewegen.

❑ **Dedizierte Server-Lösung (Dedicated Server-Network)**

In einer solchen Netzwerk-Umgebung übernehmen **die einzelnen Server genau zugewiesene Aufgaben**. Sie werden nicht mehr zusätzlich als Client (Arbeitsstationen)n eingesetzt. Dies ermöglicht ein Plus an Sicherheit, sowie eine vereinfachte Administration, ist jedoch weiterhin mit einer aufwendigen Zugriffsberechtigungsverwaltung verbunden, wenn von Seiten der Arbeitsplatzstationen auf mehrere Server zugegriffen werden soll.

❑ **Dedizierte Server-Lösung mit zentraler Verwaltung**

Diese - in großen Netzwerken einzig praktikable - Lösung betrachtet durch zusätzliche je nach Hersteller unterschiedliche Softwarekomponenten **(Domaine-Controller bei WINDOWS-NT bzw. NDS-Dienst bei NetWare) in ein Netzwerk eingebundene und ausgewählte Serverlaufwerke als logische Einheit (Domäne)**. Dies ermöglicht serverübergreifend eine Zentralisierung der Netzwerkadministration. Die Einrichtung von Nutzern, die Verwaltung von Gruppen und Netzwerkressourcen kann einheitlich gestaltet und von einem Systemadministrator durchgeführt werden.

1.2.2 Der Einsatz von Domänen bzw. NDS

Auf der Grundlage unterschiedlicher technischer Lösungen verfolgen beide Komponenten in ihrer jeweiligen Netzwerkumgebung

- Domänen - WINDOWS-NT
- NDS - NetWare

die gleiche Zielsetzung; eine erleichterte und zentrale Netzwerkadministration.

1.2.3 WINDOWS-NT und Domänen

Die Zugriffsverwaltung jedes WINDOWS-NT-Servers erfolgt mit Hilfe von **SAM (Security-Account-Manager)** und der zugehörigen Datenbank.

Bei **zentraler** Benutzerverwaltung für eine festgelegte organisatorische Einheit **(Domäne)** wird eine zugehörige **zentrale** SAM-Datenbank auf einen **zentralen** (Domänen) Server (Primary-Domänen-Controller) gepflegt. Diese regelt die Zugriffsverwaltung für alle der Domäne zugeordneten Rechner (Ressourcen).

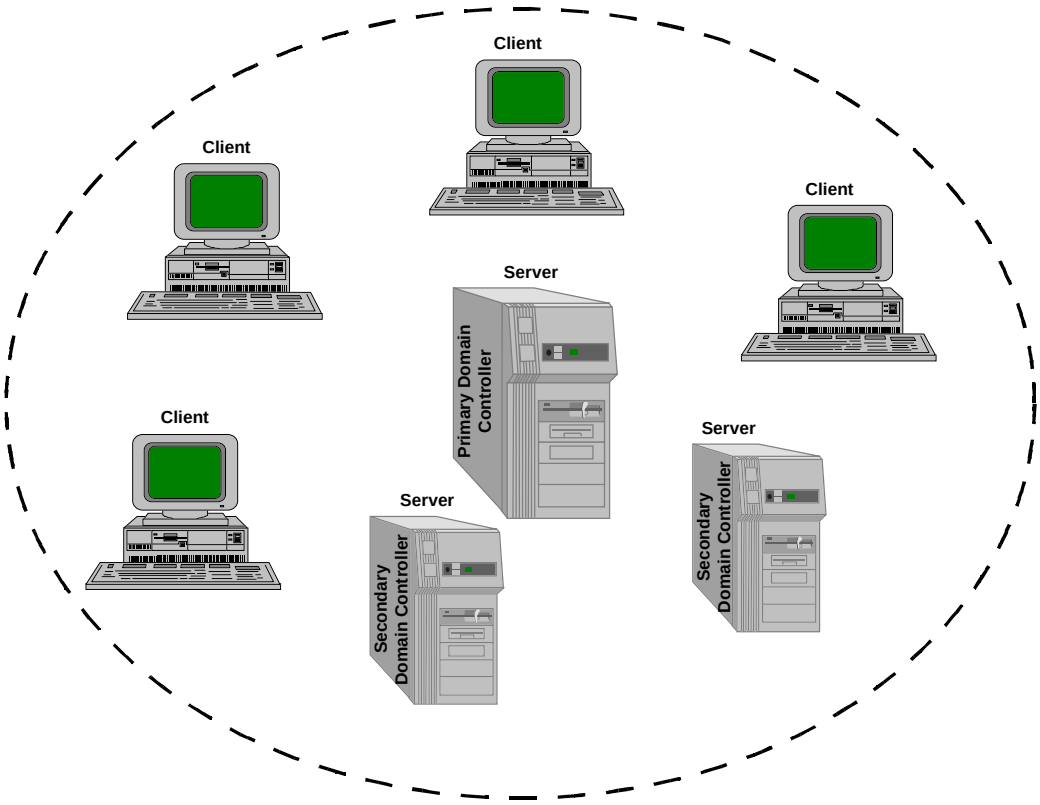

Bild 2 Domäne als Organisationseinheit von WINDOWS-NT

Weitere Server der Domäne können Kopien (für Notfälle) der SAM-Datenbank verwalten und werden dann als **"Secondary-Domain-Controller"** bezeichnet.

Die SAM-Hauptdatenbank wird regelmäßig in anzugebenden Zeitintervallen mit den Kopien synchronisiert.

Administrative Tools

Server-Manager

ermöglicht einen **Überblick über Arbeitsplatzstationen und Server sowie deren Funktionen in einer Domäne**.

In großen Unternehmen mit umfassenden organisatorischen Strukturen werden **viele Domänen** einzurichten sein. Deren Zusammenbindung erfolgt in einem äußerst komplexen Prozeß über die Erzeugung sogenannter **"Vertrauensstellungen"** (Trust Releationships).

Auf die vielfältigen Gestaltungsmöglichkeiten und die Auswirkungen auf Administration, Sicherheit und Rechteverwaltung kann an dieser Stelle nicht eingegangen werden.

Wichtig ist es zu verstehen, daß die Domänen als Organisationseinheit in einem WINDOWS-NT-Netzwerk eine einheitlich flache Struktur haben und keine weitere hierarchische Untergliederung ermöglichen. Eine dezentrale Administration und Benutzerverwaltung muß daher über eine gut vorgeplante Einrichtung von Domänen und sinnvollen Vertrauensbeziehungen realisiert werden.

Notizen:

1.2.3.1 NetWare/Novell und NDS

Eine systemweite, einfache Zugriffs- und Personenverwaltung wird von Novell mit dem **Verzeichnisdienst NDS (Novell Directory Service)** sowie der zugehörigen **NDS-Datenbank** verfolgt.

Alle in einem Netzwerk vorhandenen Objekte, wie z.B. Anwender, Rechner, Gruppen, Drukker, Platten, etc. werden innerhalb der globalen NDS-Datenbank verwaltet. Die NDS fungiert insoweit als transparentes zentrales Verzeichnis für alle Ressourcen innerhalb der Datenbank.

Unabhängig vom jeweiligen Standort, werden die einzelnen **Objekte hierarchisch und organisatorisch** strukturiert.

Verzeichnisebenen bezeichnet man als **Container** (Organizational Unit), nicht weiter untergliederte **Einzelobjekte als Blätter** (Leaf).

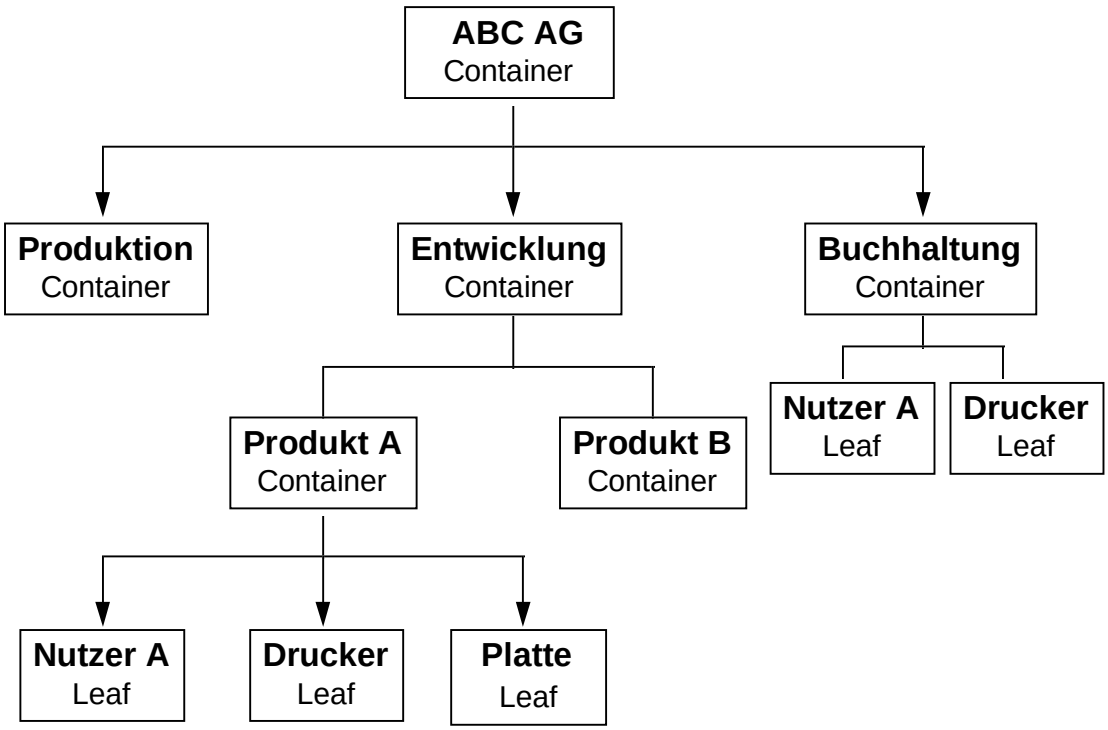

Bild 3 NDS als Strukturverwaltung unter Novell/NetWare

Mit Hilfe von **NDS** läßt sich **ein komplexes Unternehmen in einer logischen Netzwerkstruktur abbilden**. Die NDS kann als verteilte Datenbank mit Replikationen der einzelnen Partitionen auf allen Serverlaufwerken verteilt werden. Die hierzu notwendige Synchronisation mit der Master-Replikation erfolgt zeitgesteuert und automatisch.

1.2.3.2 Zusammenfassung Hardwarekomponente

Ein Netzwerk besteht jeweils aus vielen verschiedenen Hardwarekomponenten (Objekten). Für Transparenz, Strukturierung und Zugriffsverwaltung verfolgen die Hersteller z.B. mit Domain-Controller und NDS unterschiedliche Konzepte.

Zur Prüfung in einer Netzwerkumgebung bedarf es eines grundsätzlichen Verständnisses für die Konzepte und deren Zusammenhänge.

Domain - Controller

SAM - Datenbank

NDS - Datenbank

Vertrauensstellungen (Trust Releationships)

Replikationen

Container

Synchronisation

Notizen:

Fragen und Übungsaufgaben:

1) Erläutern Sie die grundlegenden Unterschiede von WINDOWS-NT und NetWare bei der Entwicklung eines Netzwerkkonzeptes?

2) Können Kopien einer SAM-Datenbank mit NDS-Replikationen verglichen werden?

3) Welche organisatorischen Einheiten finden sich in NetWare-Netzen?

4) Wie werden Verbindungen zwischen organisatorischen Sub-Einheiten von WINDOWS-NT-Netzen hergestellt?

Notizen:

2 Die Umsetzung des Client-Server-Prinzips in SAP R/3

Innerhalb des SAP R/3-Systems erfolgt eine Aufteilung der mit der Verarbeitung zentraler Daten verbundenen Prozesse in:

- die Kommunikation mit dem Anwender,
- die Verarbeitungsvorgänge der Software,
- das Datenmanagement.

Zu jeder der aufgezeigten Aufgaben wird eine Softwarelösung als Service zur Verfügung gestellt.

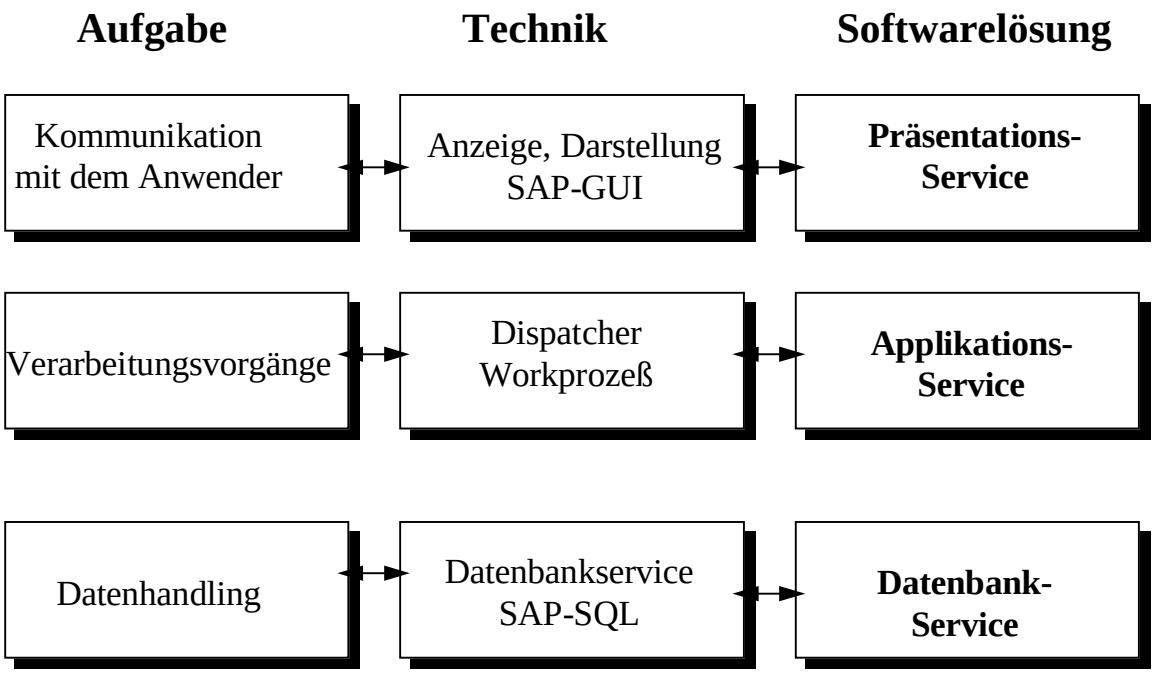

Bild 4 Softwaretechnische Darstellung einer SAP R/3-Lösung

Jeder dieser Softwareprozesse ist beliebig skalierbar und kann dementsprechend auf **unterschiedliche Hardwarekomponenten** verteilt werden. Bei ausreichend großen Maschinen ist es möglich, alle Servicekomponenten einheitlich auf einen Rechner zu legen und dort laufen zu lassen. Dies geschieht gelegentlich, z.B. bei Testsystemen.

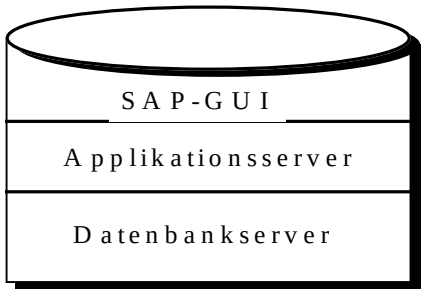

Bild 5 Umfassende Installation aller R/3-Serverprozesse auf einer Maschine

Die logische Trennung der einzelnen Servicekomponenten erlaubt es weiterhin, beliebig Hardwareerweiterungen vorzunehmen und die dargestellten **Serviceprozesse beliebig zu skalieren und auf die zusätzliche Hardware aufzuteilen**.

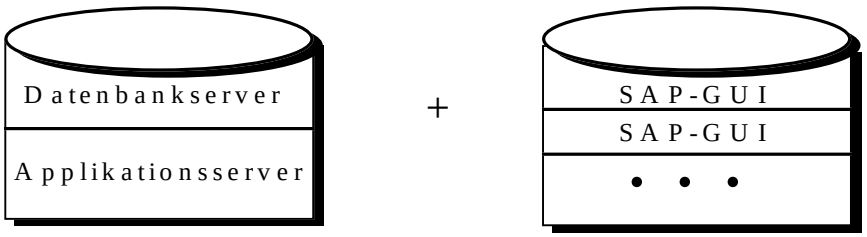

Bild 6 SAP R/3-Installation auf verteilter Hardware

Während sich der **Präsentationsservice** (soweit die Anwender über Personalcomputer als Arbeitsstationen verfügen) **auf jedem einzelnen Anwendungscomputer** befindet und der Applikationsservice auf verschiedene Serverlaufwerke aufgeteilt wird, bedient man sich aus Gründen der Datenintegrität beim **Datenbankservice häufig einer einzelnen, sehr leistungsfähigen Maschine**. Grundsätzlich ist es jedoch ohne weiteres möglich, eine einheitliche Datenbank verschiedener Hardwareservern (verteilte Datenbank) zuzuordnen.

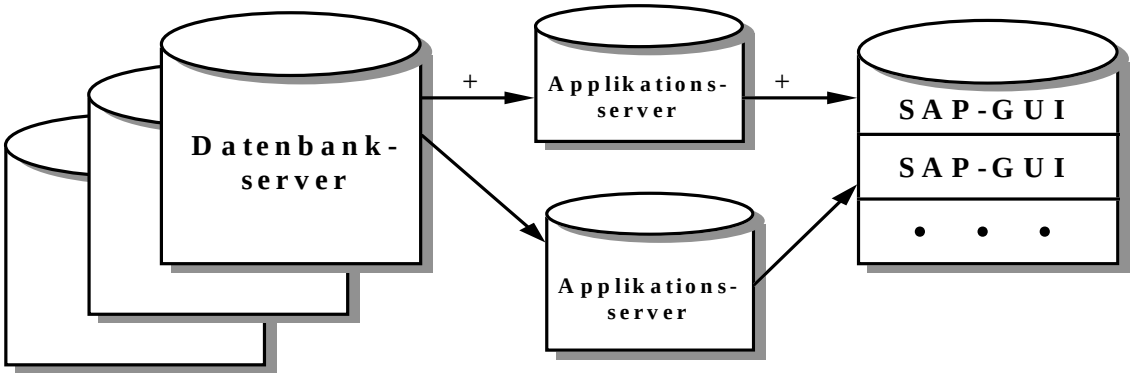

Bild 7 Skalierbarkeit der Client-Server-Prozesse im SAP R/3-System

Neben den aufgeführten verteilten Aufgaben gibt es in einer SAP R/3-Umgebung **weitere Serviceprozesse**, wie z.B.:

- Message-Server

  Informationsaustausch zwischen Servern

- Gataway-Server

  Kommunikation mit externen Systemen

- Enqueue-Server

  Verwaltung der Sperrmechanismen

- Print-Service

  Verwaltung des Print-Spools und der Ausdrucke,

die häufig dedizierten Servern, also einzelnen Geräten, zugeordnet sind.

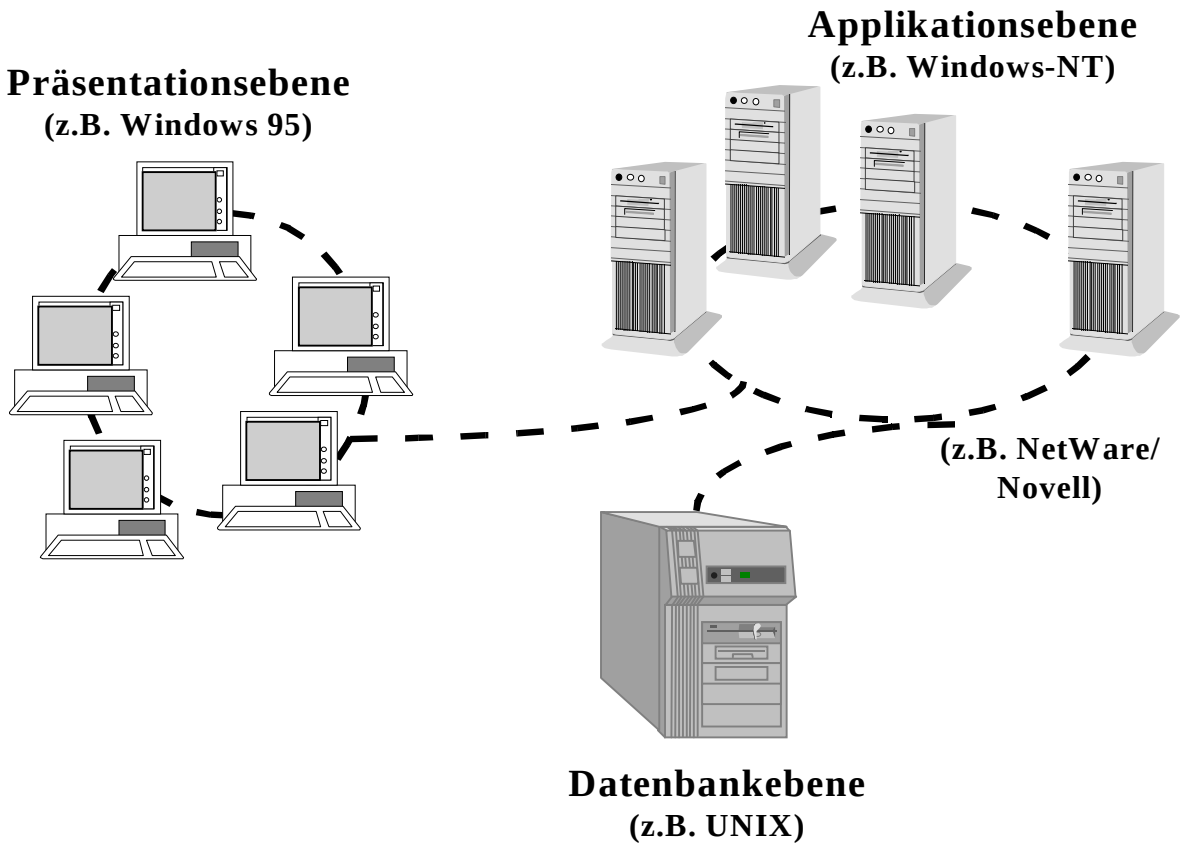

Bild 8 Modularer Aufbau und Skalierbarkeit einer SAP R/3 Lösung

Für den Revisor ist das von SAP realisierte Client-Server-Modell sowie die hiermit erreichbare **Skalierung auf nahezu beliebig viele Midrangerechner** insoweit interessant, als sich die von ihm zur Beurteilung von Hardwareschutz und Zugriffssicherheit zu **erfassende Rechnerumgebung dynamisiert**. Eine **Aussage über einen einzelnen**, sicher untergebrachten und vor unbefugtem Zugriff geschützten **Server sagt nichts über das Gesamtsystem**, zumal die in ein SAP R/3-System eingebundenen Rechnern durchaus an unterschiedlichen Standorten stehen und über ein Netzwerk kommunizieren können. Nicht mehr der einzelne Rechner, sondern der **gesamte, für das SAP-System eingesetzte Hardwarebereich** einschließlich der zugehörigen firmeninternen und öffentlichen Netzwerke **markieren das Prüfungsumfeld** und sind dementsprechend in die Überlegungen zur Revision des Systems einzubeziehen.

3 Systemunabhängigkeit einer SAP R/3-Lösung

SAP strebt mit der R/3-Lösung eine weitgehend **Systemunabhängigkeit** an. Bestimmte Aufgaben, wie z.B. die Verwaltung der **SAP-Daten** werden an die ohnehin bereits vorhandenen **relationalen Datenbanksysteme** ausgelagert. Hierbei arbeitet SAP mit jedem gängigen relationalen Datenbank- und deren Datenbankmanagement-System zusammen.

SAP ist darüber hinaus auf den gängigsten, in der **Midrange-Betriebssystemen**, wie z.B.:

- UNIX mit zahlreichen Derivaten (AIX, HP-UX, Solaris, etc.)
- WINDOWS-NT
- OS/400

lauffähig. Eine SAP-Umgebung kann aus **Servern mit unterschiedlichen Betriebssystemen** bestehen, die ihrerseits über eine zusätzlich vorhandene **Netzwerklösung**, wie z.B. NetWare/Novell **mit den Arbeitsplatzstationen kommunizieren**.

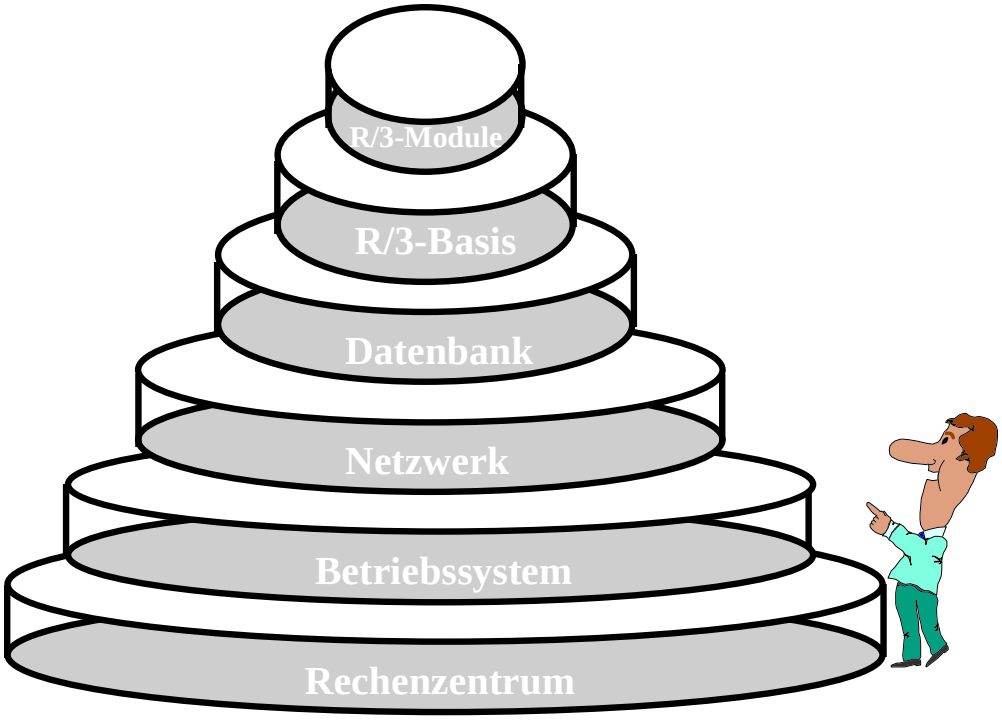

Bild 9 Schichten einer SAP R/3 EDV-Lösung

Bei einer Gesamtbetrachtung eines SAP R/3-Systems lassen sich hiernach die vorstehend aufgeführten prüfungsrelevanten Schichten identifizieren.

4 R/3 Client-Serverkonzept und die Folgen für die Revision

Der EDV-Betrieb, ehedem einem elitären Kreis von RZ-Mitarbeitern vorbehalten, hat sich, spätestens mit der **Verbreitung des Personalcomputers, demokratisiert**. In einer SAP R/3-Umgebung **sehen sich die Anwender** durchaus als **ausreichend sachverständig**, um individuelle **Datenweiterverarbeitung auf dem eigenen Personalcomputer durchzuführen**. In Verbindung mit dem problemlosen einfachen Datenaustausch zwischen Serverlaufwerk und Arbeitsplatzstation wird jeder in einem Netzwerk eingebundener Rechner zum Gefahrenpotential. Dieses reicht weit über die allseits diskutierte Virenproblematik hinaus und geht von fehlerhaften eigenentwickelten "Makro"-Programmen, über die Einspielung unautorisierter Programmstände bis zur möglichen Ausspähung und Ausschleusung vertraulicher Informationen über Disketten oder Telefonleitungen.

Die **Modularität und die damit verbundene Miniaturisierung** der Systeme verleiht der **EDV-Umgebung ungeheure Dynamik**. Eine kompetente Aussage darüber, welche Server und Arbeitsplatzstationen ein komplettes EDV-System abbilden ist nur für den Augenblick und unter Vorbehalten möglich. **Das Netz als Ganzes, einschließlich aller darin eingebundenen UNIX-, Novell- und sonstiger Server sowie der zugehörigen Arbeitsplatzstationen bildet ein sich tagtäglich änderndes Prüfungsumfeld.**

Die **Systemunabhängigkeit** des R/3-Systems hat für die Prüfung ebenfalls nachteilige Konsequenzen. **Schutz und Sicherheit** der EDV-Daten wird **von jedem Hersteller naturgemäß nur für die von ihm zu verantwortenden Bereiche optimiert**, d.h., von **SAP nur** für das **Basissystem und die Module**, vom Hersteller des hierzu notwendigen (fremden) **Datenbanksystems** nur **für seine Datenbank**, vom Hersteller der Hardware nur für das von ihm vertriebene **Betriebssystem** und vom Netzwerkhersteller nur für das Netzwerk und die **Kommunikationskomponenten**. Da für alle aufgeführten Schichten gleichermaßen komplexe, häufig objektorientierte Berechtigungskonzepte zur Verfügung gestellt werden, ist eine Beurteilung der Gesamtsicherheit und insbesondere der Interdependezen zwischen diesen verschiedenen Schichten für den EDV-Revisor außerordentlich zeitaufwendig und schwierig.

Modularität

Skalierung

Datenbanksystem

Betriebssystem

Netzwerksystem

Hardwareumgebung

Fragen und Übungsaufgaben:

1) Erläutern Sie unterschiedliche Netzwerkkonzepte mit Vor- und Nachteilen

2) Welches sind die Elemente eines R/3 Client-Server-Konzeptes?

3) Welche Service-Einheiten finden sich in einer R/3 Lösung?

4) Welche Schichten sind bei Installation einer R/3 Lösung durch die EDV-Revision zu prüfen?

Notizen:

II Kennzeichen einer "revisionsfreundlichen" EDV-Umgebung

Es gibt kein anerkanntes Gütesiegel für eine revisionsfreundliche Informationsverarbeitung. Da jedoch nahezu alle mit EDV-Hilfe abgewickelten Betriebsprozesse zu Sekundärdaten eines EDV-geführten Rechnungswesens führen, muß der EDV-Betrieb ganz allgemein die Erfüllung der aus Gesetz und Rechtsprechung abgeleiteten **GoBS** oder - spezieller - der **GoDV** sicherstellen (vgl. IDW, FAMA-Richtlinie; IIR, DV-Revision Leitfaden; Schuppenhauer, GoDV). Hinzu kommen die **Bestimmungen des Datenschutzes** und aus unternehmerischem Eigeninteresse formulierte **Sicherheits- und Schutzanforderungen** an die EDV.

Im Rahmen dieser Vorgaben muß die EDV für den Prüfer nachvollziehbar, sicher und kontrollierbar sein. Dazu zählen u.a. die:

- ❏ Dokumentation und Prüfbarkeit der in einer EDV-Umgebung vorhandenen **Hardware**,
- ❏ Dokumentation und Prüfbarkeit der verwendeten **Software**,
- ❏ Dokumentation und Prüfbarkeit des **Systembetriebes**,
- ❏ Dokumentation und Prüfbarkeit der mit der EDV-Anwendung verbundenen **organisatorischen und baulichen Gegebenheiten**.

Auf diese Punkte wird im folgenden näher eingegangen. Die in diesem Zusammenhang aufgeführten Programme stehen stellvertretend für weitere Produkte, die nicht explizit genannt sind oder geben die subjektive Erfahrung des Autors wieder.

1 Dokumentation und Prüfbarkeit der in einer EDV-Umgebung vorhandenen Hard- und Software

1.1 Aufnahme der Hardware

Kennzeichen für eine moderne EDV-Umgebung sind die für verschiedene Aufgaben in ein **Netzwerk integrierten Serverlaufwerke** sowie die dezentral angebundenen **PC-Arbeitsstationen** der einzelnen Anwender.

Ausstattung und Konfiguration dieser Rechner können sowohl die **Arbeit auf den Arbeitsplatzstationen selbst**, als auch den **sicheren Zugang und die Arbeit auf die Netzwerkserver beeinflussen**. Sehr schnell sind beispielsweise Speicherbausteine entfernt, ist die teure Bildschirmkarte gegen ein billiges Produkt aus dem privaten Computer ausgewechselt oder eine ISDN-Karte für den Internet-Zugang installiert, ohne daß man es dem jeweiligen Rechner ansieht. Darüber hinaus gehen **unberechtigte Zugriffsversuche** auf EDV-Anwendungen oft von schlecht abgesicherten Arbeitsplatzstationen aus. Dieses macht laufende Prüfungen in diesem Bereich notwendig.

Revisionsfreundlich ist eine EDV-Umgebung, deren einzelne Rechner und Rechnerkomponenten sowohl in Papier- als auch in Dateiform dokumentiert sind. Diese, als **Hardwareinventarisierung** bezeichnete Zusammenstellung erleichtert zudem die Unterstützung der Anwender, die Fehlerdiagnose und ist eine der Grundlagen für die Beurteilung des Supportaufwandes.

Die Führung eines entsprechenden **Hardwareinventars ist Aufgabe der Systemadministration**. Liegt es nicht vor, so kann der Revisor die für seine Prüfung notwendigen Informationen mit Hilfsprogrammen im Bereich des Netzwerkmanagements, wie beispielsweise

- Dr. Solomon's Audit 2.5, Dr. Solomon, D,
- TRACK-IT, Blue Ocean Software, USA,
- Auditor Version 1.4, Prax Soft, UK,
- Barefoot Auditor, Pathfinder, UK,
- INTEGRA SME, SNI, D,
- NetCensus, Tally Systems, D,
- SiteInventory, McAfee, D,

zusammenstellen und auswerten.

Die Hardwareinventur erfolgt, sobald sich die Anwender innerhalb des Netzwerkes anmelden, automatisch. Die wichtigsten Inhalte einer entsprechenden **Aufnahme** (Computerart, BIOS, Betriebssystem, Hauptspeichervolumen, Festplatte, Schnittstellen, Netz-, ISDN- und Grafikkarten) sollten von Zeit zu Zeit gegen d**en aktuellen Hardwarestand im Hinblick auf Veränderungen abgeglichen werden**.

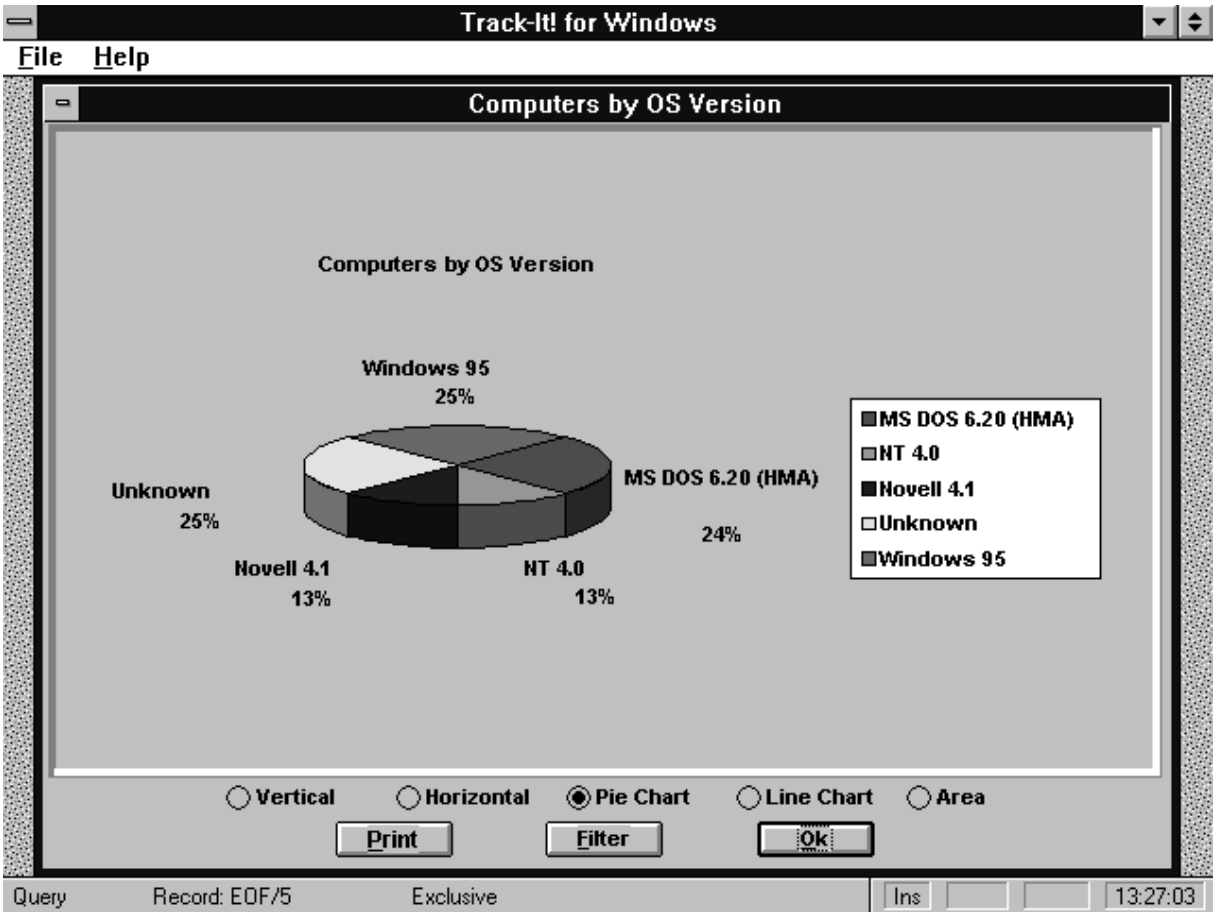

Bild 10 Hardwareinventur und -analyse mit Hilfe von "TRACK-IT"

Von den Arbeitsplatzstationen ausgehendes Gefahrenpotential wird erheblich reduziert, wenn der **Datenaustausch ausschließlich firewallgeschützten (E-mail, ISDN) Serverkomponenten** übertragen und außer dem Netzstecker alle hierfür geeigneten Laufwerkschächte und Schnittstellen an den Arbeitsstationen ausgebaut oder abgeschaltet werden.

1.2 Aufnahme der Software

Neben der Hardware sind die in einer EDV-Umgebung eingesetzten Programme Prüfobjekte für den EDV-Revisor. Dies gilt besonders in einer Netzwerkumgebung. Die grundsätzlich bestehende Gefahr, daß einzelne Anwender und Abteilungen **unautorisierte Programme** auf ihren PC-Arbeitsstationen verwenden ist durch regelmäßige Kontrollen zu verringern. Hierdurch mögliche Schäden sind für die betroffenen Unternehmen nicht unerheblich und gehen weit über das im Vordergrund stehende Virenproblem hinaus. Unsauber programmierte Software führt u.U. zu Systemabstürzen im Netz. Nicht definierte Schnittstellen und fehlerhafte Software kann zu Datenverlusten und falschen Ergebnissen führen. Die Anwendung nicht lizensierter Programme schadet dem Ruf eines Unternehmens und zieht ggf. Schadensersatzansprüche nach sich.

Revisionsfreundlich ist eine EDV-Umgebung, welche mit einer **aktuellen und detaillierten Aufzeichnung** für den Betrieb autorisierten und **lizensierten Programme** in Schrift- und Dateiform betrieben wird.

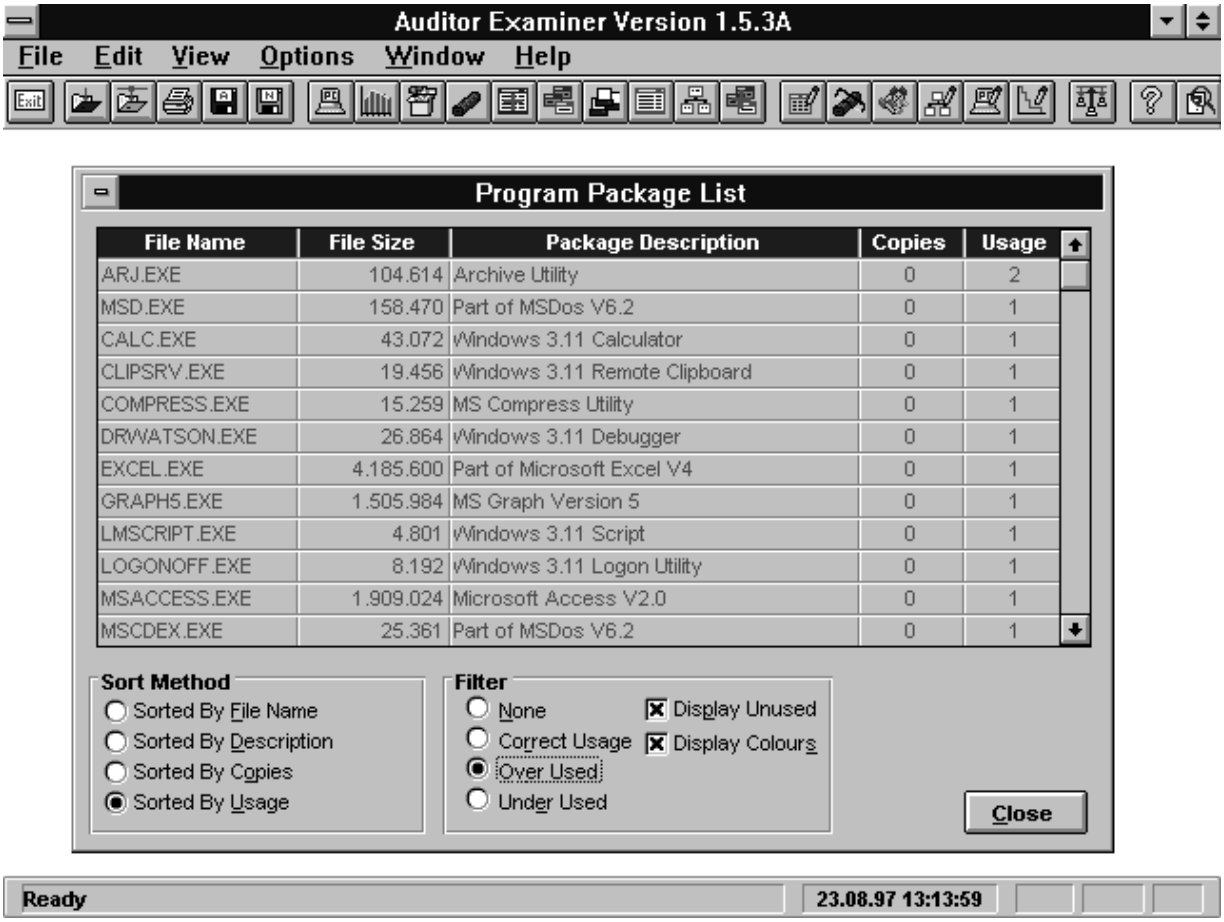

Bild 11 Softwareinventur und -analyse mit Hilfe von "Auditor Examiner"

Die Führung eines solchen **Softwareinventars als Maßstab für die nachfolgende Suche nach Abweichungen**, ist ebenfalls originäre Aufgabe der Systemadministration. Hierauf spezialisierte Programme werden für die zentrale Installation und das Update vorhandener Programme auf den Arbeitsplatzstationen sowie die Lizenzüberwachung der Netzwerksoftware eingesetzt. **Der Prüfer kann sich dieser Programme bedienen oder die bereits bei der Hardwareaufnahme bezeichnete Software verwenden.**

2 Dokumentation und Prüfbarkeit des Systembetriebes

2.1 Einführung

Die Sicherheit und Integrität der Datenbestände in einer heterogenen EDV-Umgebung können durch vielfältige Einflüsse, wie bspw.:

- Stromausfall,
- fehlerhafte Installation,
- fehlerhafte programmierte Software,
- schadhafte Leitungen,
- Hardwarefehler
- oder Programmanipulationen,

beeinträchtigt werden. Die EDV-Revision muß sich deshalb davon überzeugen können, ob die einzelnen **Schichten einer EDV-Umgebung mit Hardware, Betriebs- und Kommunikationssystem sowie Datenbank und die hierauf aufbauenden Programme stabil ablaufen**, auftretende Fehler umgehend beseitigt werden und - nach einem Systemausfall - eine schnelle, unkomplizierte Wiederinbetriebnahme einschließlich einer Rekonstruktion beschädigter Datenbestände möglich ist.

Alle Betriebssysteme bieten spezielle Funktionen, die den laufenden Systembetrieb, einschließlich dabei auftretender Fehler, automatisch in **Logdateien** erfassen, vorausgesetzt, diese Funktionen wurden aktiviert. **Eine revisionsfreundliche Gestaltung des EDV-Betriebes schreibt diese Aktivierung zwingend** vor und stellt dem EDV-Revisor neben den hieraus resultierenden **Protokollen** eine Übersicht zur Verfügung, in der die Bedeutung und Auswirkung der einzelnen, häufig vorkommenden Fehlermeldungen hinsichtlich Datenschutz und -sicherheit detailliert erläutert werden.

Die laufende Kontrolle und Interpretation der Fehlermeldungen sowie die Analyse des Sicherheitsstatus von Betriebs- und Datenbanksystemen wird durch Zusatzprogramme, wie sie speziell für die Revision angeboten werden, wesentlich vereinfacht.

2.2 Analysen auf Großrechnerebene

Revisionsseitige Anforderungen an Datenschutz- und Sicherheit werden auf der **Großrechnerseite** seit langem durch leistungsfähige Produkte unterstützt. **Schutzsysteme, wie z.B. RACF und ACF2** sowie zusätzliche Schutzmechanismen in den Anwendungsprogrammen ermöglichen grundsätzlich eine zuverlässige Absicherung der auf dem Host gespeicherten Daten und Programme. Der **Systembetrieb** wird darüber hinaus durch **SMF** (System Management Facilities) und **systeminterne Logs laufend und im Detail dokumentiert**. Er bleibt damit transparent und nachvollziehbar.

Trotz dieser guten Absicherung gibt es eine Reihe von Gründen, auch den **Systembetrieb** eines Großrechners **regelmäßigen Kontrollen** zu unterziehen. Insbesondere die recht **komplexe Zugriffsverwaltung unter RACF** führt häufig dazu, daß Anwender, um sie in ihren Arbeiten nicht einzuschränken und den Administrationsaufwand in überschaubarer Größenordnung zu halten, mit global zugeteilten Zugriffsberechtigungen und damit **zu großem Zugriffsberechtigungsumfang** arbeiten.

Der EDV-Prüfer kann sich, z.B. durch eine **Analyse der in RACF vorgenommenen Sicherheitseinstellungen**, durch die von diesem System generierten **Reports und der SMF-Records sowie der sonstigen Logdateien** davon überzeugen, daß das Großrechnersystem mit einem guten Sicherheitsstandard betrieben wird. Eine zentrale Zusammenschau aller für ihn notwendigen Informationen wird jedoch nicht angeboten.

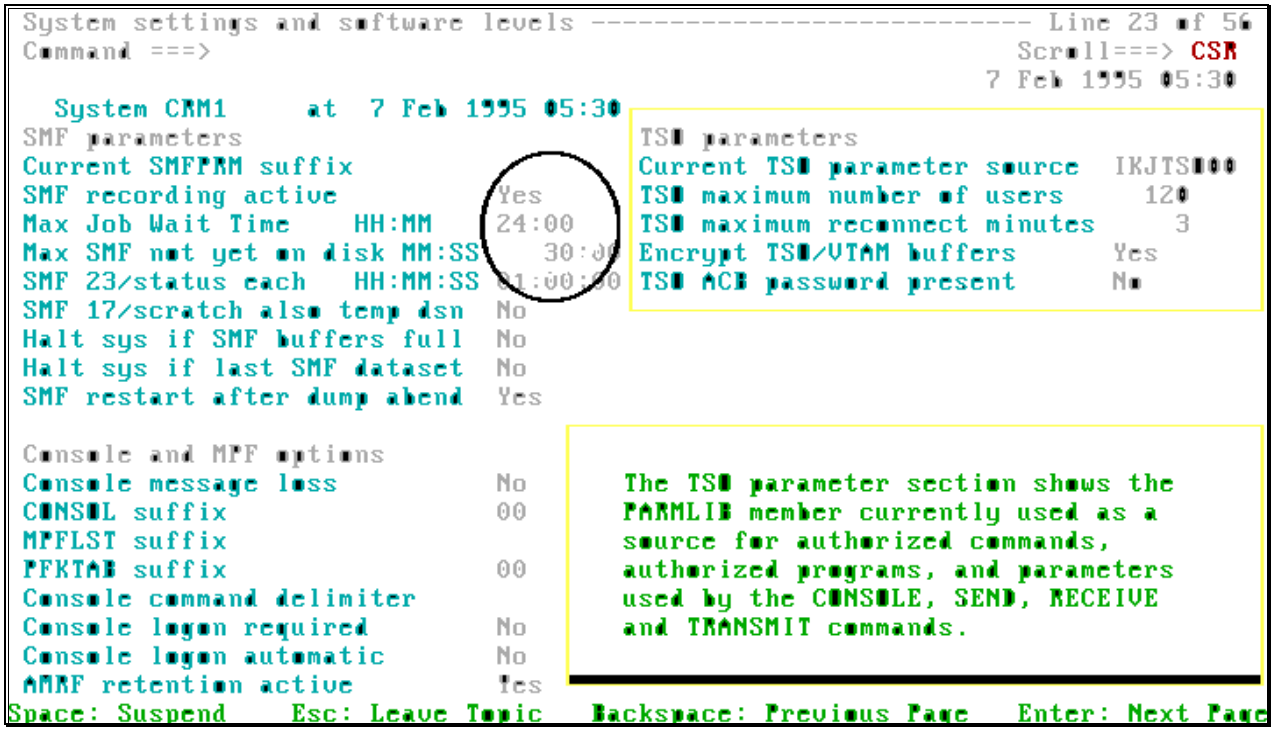

Bild 12 Analyse eines IBM-Host-Betriebes mit Hilfe von "CONSUL/Audit"

Programme, welche die systemseitige Prüfung auf Großrechnerseite wesentlich erleichtern und sehr schnell einen Überblick ermöglichen, sind **CONSUL/Audit für RACF (ACF2)** und **EKC Tools für ACF2 und RACF**. Alle für die Systemsicherheit relevanten Parameter und Tabellen, Sicherheitseinstellungen zu den Bibliotheken, Programmen und Anwendern sowie Auffälligkeiten aus dem laufenden Systembetrieb werden online dargestellt oder als Liste ausgedruckt.

2.3 Analysen auf Midrange(UNIX)-Systemen

Mit der Suche nach einem **hardwareabhängigen Standardbetriebssystem für Midrangerechner** hat das Mitte der sechziger Jahre an amerikanischen Universitäten entwickelte **UNIX** weltweit an Bedeutung gewonnen. Mittlerweile verfügt jedes größere Unternehmen über mindestens einen UNIX-Server. Es handelt sich mit allen seinen Derivaten um eine der wesentlichen **Plattformen für das weltweit verbreitete SAP R/3-System**.

Als **universitäres**, für den **technischen Bereich** entwickeltes und **offenes Betriebssystem** stand UNIX nicht ganz zu Unrecht in dem Ruf, lediglich mit **mangelhaften Sicherheitsmechanismen** ausgestattet zu sein. Dieses hat sich erst in den letzten Jahren mit der **Sicherheitszertifizierung neuerer UNIX-Versionen** geändert. Trotzdem bleibt eine UNIX-basierte Rechnerumgebung für den EDV-Revisor problematisch.

Typischerweise stehen in einem Unternehmen für jede komplexere Anwendung mindestens **ein oder mehrere Server** zur Verfügung, **die über Leitungen kommunizieren**. Größere Unternehmen verfügen über mehrere solcher **Subsysteme, die sie über ein Netzwerk verbinden**. Zuletzt erfolgt die Einbindung von Händlern und Lieferanten bzw. die **weltweite Öffnung durch Integration des Internet**.

Die Prüfung in einem derart komplexen System mit einer großen Anzahl von Gruppen, hunderten von Anwendern und tausenden von Dateien, bedarf eines Softwarewerkzeuges, welches unkompliziert und schnell zur Beurteilung der DV-Sicherheit beiträgt.

Ein einfaches und effizientes Programm ist **PC-UNIX Audit**. Es handelt sich um eine **DOS- und WINDOWS-Entwicklung**, die **- unabhängig von dem verwendeten UNIX-Derivat -** vier auf nahezu jedem UNIX-System vorhandene Dateien

- Paßwort-File,
- Group-File,
- Shadow-Paßwort-File,
- Directory-File

einliest und unter Revisionsgesichtspunkten auswertet. Das Programm analysiert den Sicherheitsstandard des verwendeten Servers unter Berücksichtigung der verwendeten UNIX-Version.

Die durchgeführten Analysen sind umfassend und reichen von **mangelhaften Systemeinstellungen, Anwendern ohne Paßwörter** oder mit problematischen Rechten bis zu **ungeschützten Systemdateien** und ähnlichen Dingen.

Weitere für die Analyse von UNIX-Systemen **interessante Programme**, wie z.B.:

- COPS (Computer ORACLE and Paßwort System), Public Domane, UK,
- RAXCO Security Toolkit, UK,
- SecurMax, Open Vision, UK.

sind teilweise kostenfrei erhältlich.

2.4 Analyse von WINDOWS-NT-Umgebungen

2.4.1 Grundsätzliches zu WINDOWS-NT

WINDOWS-NT wurde von Microsoft **zunächst als Arbeitsplatz-Betriebssystem** entwickelt. **Ziel** war es, die auf Großrechnerebene bereits seit langem gängigem und für kaufmännische und technische Anwendungen notwendigen **Sicherheitsstandards** zu implementieren. Insoweit wird von Fachleuten einhellig die Meinung vertreten, daß Microsoft mit **WINDOWS-NT** ein erstes, unter Sicherheits- und Schutzaspekten **ernst zu nehmendes Betriebssystem** auf den Markt gebracht hat.

Um WINDOWS-NT neben gängigen Netzwerkbetriebssystemen, wie z.B. NetWare/Novell zu etablieren, wurde es mit **zusätzlichen Netzwerkfunktionalitäten** ausgestattet. Dementsprechend werden zwei Systeme

- WINDOWS-NT Workstation (Arbeitsplatzstation)
- WINDOWS-NT Server (Netzwerkstation)

zur Verfügung gestellt.

Grundsätzlich unterscheiden sich beide Systeme nur insoweit, als die mit dem (Netz-) Serverbetrieb notwendige zusätzliche Funktionalität aus einem Einplatzsystem mit wenigen Handgriffen generiert werden kann.

Nachfolgend wird im wesentlichen auf **Schutz und Sicherheit der Netzwerkvariante** von WINDOWS-NT eingegangen.

2.4.2 Elemente eines Schutz- und Sicherheitskonzeptes

Prüfungsansätze ergeben sich für den EDV-Revisor eines Netzwerkbetriebssystems bei dessen Schutz- und Sicherheitsmechanismen, den Schlössern, die es vor unberechtigten Zu- und Eingriffen schützen und den laufenden Betrieb dokumentieren.[1]

❏ **Identifizierung von Anwendern**

Sowohl auf eine Arbeitsplatzstation als auch das Netzwerk sollen ausschließlich hierzu **autorisierte Anwender** zugreifen.

Die Kontrolle einer entsprechenden Autorisierung setzt voraus, daß der entsprechende Mechanismus innerhalb des Betriebssystems aktiviert ist. Nur dann erfolgt ein sogenanntes Logon, d.h., es wird ein Anmeldevorgang notwendig. Hier muß sich der Nutzer zu erkennen geben. Dieses kann hardwaretechnisch durch sogenannte Security-Cards erfolgen, wobei der Rechner die erforderlichen Angaben aus einem Kartenchip oder einem Magnetstreifen ausliest. In den meisten Fällen jedoch, wird die **Autorisierung durch Eingabe eines Anwendernamens sowie eines zugehörigen Paßwortes** abgefragt.

Weiteres Element der Identifizierung in einem WINDOWS-NT-System ist der dort gespeicherte **Benutzerstammsatz** in dem alle relevanten Informationen, wie z.B. der Benutzername, Paßwort, ggf. **Arbeitsplatzstation, Gruppenzugehörigkeit und Zugriffszeiten** gespeichert sind.

[1] Vergleiche Christoph Fischer, Netzwerksicherheit, Unveröffentlichte Vortragsunterlagen

❏ **Rechteverwaltung**

Das Sicherungskonzept in einem WINDOWS-NT-System ist (ebenso wie bei SAP R/3) objektorientiert. **Jedes Objekt (Ressource) kann differenziert vor unberechtigtem Zugriff und vor Änderung geschützt werden.** Zentrales Element dieses Schutzsystems ist die sogenannte **Access-Control-List** (ACL), in der genau definiert ist, welcher Benutzer mit welchen Rechten auf welchen Ressourcen zugreifen kann.

❏ **Systemverwaltung/Monitoring**

Das Betriebssystem bedarf, ebenso wie das SAP-Basissystem der laufenden Überwachung und Verwaltung. Von den hierfür zuständigen Administratoren sind Nutzer einzurichten, zu ändern und zu entfernen. Das **SAP-System** stellt sich hierbei **als einer der Nutzer des Betriebssystems** dar. Weiterhin sind Fehlfunktionen und Betriebsstörungen zu beheben, neue Server einzurichten, Drucker- und sonstige Ressourcen anzupassen.

Mit dem beschriebenen, notwendigen Aufgaben, sind weitreichende Berechtigungen (und Gefahren) verbunden. Der Systembetrieb muß transparent und für den EDV-Revisor nachvollziehbar bleiben. Auf die an dieser Stelle durch WINDOWS-NT zur Verfügung gestellten Funktionen wird an späterer Stelle eingegangen.

❏ **Kommunikationsumgebung (Connectivity)**

Jedes Netzwerk ist heute grundsätzlich mit der Möglichkeit ausgestattet, über Telefon- oder Datenleitungen beliebige Verbindungen nach außen mit anderen Rechnern oder Netzwerken aufzubauen und Daten sowie Programme auszutauschen. Beliebt ist die Möglichkeit, von außen über sogenannte **RAS (Remote Access)-Verbindungen** auf das System zuzugreifen und die dortigen Ressourcen zu nutzen. Von wesentlicher Bedeutung ist ebenfalls der **Zugriff und die Datenübermittlung über das weltumspannende Internet**.

Wesentliches Sicherheitselement einer WINDOWS-NT-Netzwerklösung ist die Abschottung nach außen über **dedizierte Kommunikations- bzw. Gataway-Server**, die Realisierung von **Firewall-Konzepten** sowie die Vermeidung ungesteuerter Kommunikation über "wilde" Modems oder ISDN-Verbindungen.

❏ **Abschottung der Arbeitsplatzstationen**

Jede Arbeitsplatzstation in einem Netzwerk birgt - wie bereits erläutert - ein nicht unerhebliches Gefahrenpotential. Die Einschleusung unautortisierter Programmstände über geöffnete **Disketten- oder CD-ROM-Laufwerke bzw. über die serielle oder parallele Schnittstellen** kann ohne weiteres zur Verbreitung von Viren sowie zu Fehlfunktionen auf den Servern führen. Dies verlangt einen regelmäßigen Einsatz aktueller Virenscanner, sowohl auf den Serverstationen, als auch den Workstations. Die Workstations sollten darüber hinaus über **keine vom Anwender beeinflußbare Schnittstelle** verfügen und der Administrator selbst sollte, da er mit seiner umfassenden Berechtigung ein ständiges latentes Gefahrenpotential für Datendateien und Programme darstellt, bei Nicht-Administrator-Aufgaben mit einer in den Rechten eingeschränkten Nutzerkennung arbeiten.

❏ **Netzwerküberwachung**

WINDOWS-NT verfügt über umfangreiche **Absicherungs- und Protokollierungsmöglichkeiten**, die von dem EDV-Revisor verwendet werden können, um den Systembetrieb zu prüfen. Die Zusammenstellung aller Daten und die Beurteilung des Sicherheitsstands ist allerdings, auch bei Einsatz der hier zur Verfügung stehenden Werkzeuge, mit erheblichem zeitlichem Aufwand verbunden. Darüber hinaus kann ein umfassendes Auditing gegen Bestimmungen des Datenschutzes verstoßen.

Die Elemente des WINDOWS-NT-Sicherheitssystems sowie die hier hinter stehenden Werkzeuge, Einstellungen und Ausgaben werden im folgenden näher erläutert.

ACL-Access Control List

Identifizierung der Anwender

Systemverwaltung

Connectivity

Netzwerküberwachung

2.4.3 Die Überwachung des Systembetriebs

2.4.3.1 Übersicht

Vor Überwachung des Systembetriebs stellt WINDOWS-NT verschiedene Optionen zur Verfügung, die wie folgt aufgegliedert werden können:

- **Security-Log**

  Aufzeichnung von Ereignissen und Vorgängen einzelner Benutzer bzw. Benutzergruppen oder Domänen

- **Systemlog**

  Aufzeichnung von systemnahen Ereignissen, wie z.B. der Startprofile und sonstiger Systemdienste

- **Application-Log**

  Aufzeichnung von Meldungen und Ereignissen, die im Zusammenhang mit dem Betrieb von WINDOWS-NT-Programmen bzw. dem Datenbanksystem angefallen sind

und auf die nachfolgend näher eingegangen wird.

2.4.3.2 Security-Log

2.4.3.2.1 Die Überwachung von Domänen

Die **Aufzeichnung von Ereignissen zu Domänen** setzt voraus, daß die entsprechende Option im **Benutzermanager** aktiviert wurde. Zur Kontrolle muß dort der Menüpunkt **POLICIES** aufgerufen und die Option **"AUDIT THESE EVENTS"** aktiviert werden.

Standardmäßig werden die nachfolgenden Ereignisse

- **Logon and Logoff**

  Aufzeichnung erfolgreicher bzw. gescheiterter Zugriffsversuche einschließlich Zeiteinträge,

- **File and Object Access**

  Protokollierung von Verzeichnis- oder Dateizugriffen, **sofern** im Dateimanager (Explorer) der Überwachungsmechanismus aktiviert wurde, bzw. Protokollierung von Druckaufträgen, **soweit** im Druckmanager hierzu der Überwachungsbefehl eingetragen ist,

- **Use of User Rights**

  Protokollierung der Verwendung anwenderspezifischer Zugriffsberechtigungen,

- **User and Group Management**

  Protokollierung von Änderungen an Anwendern bzw. Gruppen,

- **Security Policy Change**

  Aufzeichnung der Änderung von Sicherheitseinstellungen und Benutzerrechten,

- **Restart, Shutdown, and System**

  Überwachung von Ereignissen zur Systemsicherheit, insbesondere das Starten und Herunterfahren von Rechnern,

- **Process Tracking**

  Protokollierung des Aufrufs von Programmen, sowie des Mehrfachzugriffs,

aufgezeichnet.

2.4.3.2.2 Überwachung von Dateien und Verzeichnissen

WINDOWS-NT unterstützt grundsätzlich ein DOS-kompatibles (FAT) sowie alternativ ein weitergehendes NTFS-Dateisystem. Die Überwachung der Verzeichnisse und Dateien mit den WINDOWS-NT-Aufzeichnungsmechanismen setzt voraus, daß das erweiterte **NTFS-Dateisystem installiert ist**.

Die Überwachungsfunktion wird wie folgt ausgewählt und eingestellt:

Aufruf des Dateimanagers (Explorer)

Verzeichnis bzw. Datei markieren

Rechte Maustaste betätigen

Properties

Security

Auditing

Directory Auditing oder
File Auditing

Für das **Directory Auditing** stehen grundsätzlich drei Optionen zur Verfügung:

- Replace Auditing on **Subdirectorys (mit** Replace Auditing on existing Files)

  Überwacht werden alle Ereignisse für das ausgewählte Verzeichnis einschließlich der zugehörigen Unterverzeichnisse und aller zugehörigen Dateien

- Replace Auditing on **Subdirectorys (ohne** Replace Auditing on existing Files)

  Die Überwachung bezieht sich ausschließlich auf das ausgewählte Verzeichnis und seine Unterverzeichnisse ohne die jeweils zugehörigen Dateien

- Replace Auditing on existing **Files (ohne** Replace Auditing on Subdirectorys)

  Die Überwachung bezieht sich nur auf die ausgewählte Verzeichnisebene, einschließlich der hierin befindlichen Dateien.

Die weiter aufgeführten **Aufzeichnungsalternativen beziehen sich auf die Rechte**, die auf Datei- und Verzeichnisebene vergeben werden können. Einzelheiten ergeben sich aus den nachfolgenden Grafiken.

	"Eigentümer" Verzeichnis ändern	Verzeichnis Löschen	Berechtigungen für Verzeichnis ändern	Berechtigungen für Verzeichnis anzeigen	In Unterverzeichnis wechseln	Verzeichnis und Dateien erstellen	Attribute ändern	Dateiname anzeigen	Attribute anzeigen
READ				X				X	X
Write				X		X	X		
EXECUTE				X	X				X
DELETE		X							
Change Permission			X						
Take Ownership	X								

Bild 13 Alternativen zur Aufzeichnung auf Verzeichnisebene

	"Eigentümer" Datei ändern	Datei Löschen	Zugriffsberechtigungen für Datei ändern	Programm aufrufen	Daten oder Datei ändern	Dateiattribute ändern	Berechtigungen und Eigentümer anzeigen	Datei lesen	Dateiattribute anzeigen
READ							X	X	X
Write					X	X	X		
EXECUTE				X			X		X
DELETE		X							
Change Permission			X						
Take Ownership	X								

Bild 14 Alternativen zur Aufzeichnung auf Dateiebene

2.4.3.2.3 Überwachung von Druckervorgängen

Die Überwachung der druckernotwendigen Einstellungen werden innerhalb des WINDOWS-NT-Printmanagers vorgenommen.

Dateimanager (Explorer) öffnen

Eintrag NETWORK NEIGHBORHOOD auswählen

Verzeichnis PRINTERS öffnen

Gewünschten Drucker markieren

Rechte Maustaste betätigen

Properties

Security

Auditing

In dem nun geöffneten **Menü Printer Auditing** können alle für die Aufzeichnung beim Druck gewünschten Ereignisse **bezogen auf einzelne Benutzer oder Benutzergruppen** eingetragen werden. Zunächst ist der entsprechende Benutzer oder die gewünschte Benutzergruppe hinzuzufügen bzw. zu markieren. Hiernach können die nachfolgenden Überwachungsalternativen gewählt werden:

- **Print**

  Aufzeichnung der Druckaufträge, die von einem ausgewählten Benutzer bzw. einer Benutzergruppe abgesetzt werden

- **Full control**

  Festhalten von Änderungen, Anhalten u.ä. Ereignissen zu Druckaufträgen

- **Delete**

  Aufzeichnung des Anwenders, der einen Drucker gelöscht hat

- **Change permissions**

  Bezogen auf einen Einzeldrucker (Druckerobjekt) können individuelle Rechte vergeben werden. Deren Änderung wird an dieser Stelle aufgezeichnet

- **Take ownership**

  Die Zuordnung von Objekten, wie z. B. an dieser Stelle einem Drucker, erfolgt immer zu demjenigen, der dieses Objekt (Drucker) eingerichtet hat. Wird die sogenannte "Eigentümerschaft" zu einem Objekt bzw. einem Drucker geändert, so erfolgt an dieser Stelle ein Eintrag in die Logdatei

Ebenso wie bei den vorherigen Überwachungsobjekten, bzw. den Dateien und Verzeichnissen, erfolgt die Überwachung von Druckereignissen, wenn innerhalb AUDIT POLICY der Bereich FILE AND OBJECT ACCESS für die Domänen aktiviert ist.

2.4.3.3 Weitere Logdateien

System- und Application-Log bieten im wesentlichen Informationen für die Netzwerkadministration. Soweit sich hieraus prüfungsrelevante Hinweise ergeben wird darauf an späterer Stelle eingegangen.

Über die aufgezeigten Logdateien hinaus gibt es zwei weitere Bereiche, die sogenannten Dial Ports sowie die sonstigen Schnittstellen, deren Aktivitäten, z.b. im Hinblick auf ungerechtfertigte Zugriffe überwacht werden sollten.

Die Überwachung setzt voraus, daß in der Registry-Datei die Protokollierungsparameter für die entsprechenden Schnittstellen gesetzt sind.

Hierzu ist zunächst der Registry-Editor zu laden. Dieser wird i.d.R. manuell aus dem Verzeichnis %SystemROUTE%\System32 mit der Bezeichnung RACKIDT32.EXE aufzurufen sein. Hiernach werden eine Reihe von Schlüsseln aufgezeigt. Interessant sind die Schlüssel für den lokalen Rechner.

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP

  Notwendiger Parameter 0x1

- HKEY_LOCAL-MACHINE\SYSTEM\CurrentControlSet\Service\RasMan\Parameter

  Notwendiger Parameter 0x1

Aufgezeichnet werden die entsprechenden Aktivitäten in den Dateien PPP.LOG und DEVICE.LOG. Sie befinden sich standardmäßig im Verzeichnis

C:\WINNT35\SYSTEM\32\RAS

Sie sollten regelmäßig im Hinblick auf ungewöhnliche Aktivitäten kontrolliert werden.

2.4.3.4 Das Auswertungswerkzeug für Log-Dateien

WINDOWS-NT bietet mit dem **EVENT VIEWER** ein eigenes, ausgefeiltes Werkzeug, um die in den Logdateien generierten Informationen in einer strukturierten und für den EDV-Revisor interessanten Weise auszuwerten.

Logdateien können in **einem eigenen Format mit dem Suffix EVT verschlüsselt gespeichert** werden. Sie sind hiernach nur über EVENT VIEWER lesbar. Bei einer differenzierten Zuordnung der Rechte auf diese Datei, z.B. auf das Securitylog, können ohne weiteres auch datenschutzrelevante Ereignisse aufgezeichnet und **ausschließlich vom EDV-Revisor** und nicht von der Administration ausgewertet werden.

Nach Aufruf des EVENT VIEWERS kann der EDV-Revisor zunächst die für ihn interessante Domäne bzw. den gewünschten NT-Server

SELECT COMPUTER

Domäne/Server markieren

Log

Security Log
Application Log
System Log

sowie die gewünschte Logdatei auswählen. Eine weitere Eingrenzungsmöglichkeit, um die Betrachtung ausschließlich auf bestimmte Ereignisse zu lenken, erhält der Prüfer mit

VIEW

Filter Events.

Bei dem sich öffnenden Menü kann nun eine **Auswahl über Datum, Uhrzeit, Typ der Aufzeichnung** bis hin zum Anwender und Computer, auf dem das Ereignis eingetreten ist, vorgenommen werden.

Die in der Logdatei vorhandenen Informationen werden darüber hinaus mit **grafischen Symbolen** dargestellt, die die Orientierung erleichtern und folgende Bedeutung haben:

- **Information**

  Ereignis ohne prüfungsrelevante Bedeutung

- **Warnung**

  Hinweis auf einen nicht kritischen Fehler

- **Kritischer Fehler**

  Hierbei ist ein Fehler aufgetreten, der die Integrität der auf dem Serverlaufwerk bewegten und aufbereiteten Daten beeinträchtigen könnte und unbedingt behoben werden muß

- **Erfolgreiche Prüfung**

  Hinweis auf ein Sicherheitsereignis, wie z.B. der Aufruf einer geschützten Datei bzw. der An- und Abmeldung, die erfolgreich abgeschlossen wurde

- **Fehlgeschlagene Überprüfung**

  Hinweis auf ein sicherheitsrelevantes, fehlgeschlagenes Ereignis, wie z.B. der unautorisierte Zugriff auf eine geschützte Ressource bzw. die fehlerhafte Anmeldung an eine Arbeitsplatzstation

Zu den für die Revision interessanten Ereignissen können nähere Informationen angefordert werden, in dem der entsprechende **Text markiert und durch Doppelklick** eine weitere Erläuterung aufgerufen wird.

Die in einer Logdatei niedergelegten Ereignisse beinhalten u.a. die nachfolgenden Informationen:

- **Datum und Uhrzeit** des Ereignisses
- **Source**:
  Komponenten bzw. Schutzobjekt, durch welches das Ereignis protokolliert wurde
- **Kategorie:**
  thematische Einordnung des Ereignisses
- **Event:**
  Numerierung aller Ereignisse zu deren eindeutiger Identifikation
- **Benutzerkennung**, unter der das Ereignis erfolgte
- **Computername**, wo das Ereignis aufgetreten ist

Für den EDV-Revisor interessant ist die Option, Logdateien

Log

Clear all Events

zu löschen. Er sollte im Rahmen seiner Prüfung kontrollieren, wer die **Löschberechtigung für die Logdateien** besitzt, ob es für die Sicherung der Logdateien eingeregeltes und nachvollziehbares Verfahren gibt und ob diese regelmäßig, z.B. im Hinblick auf den Zugriff besonders geschützter Ressourcen bzw. fehlerhafte Login-Versuche ausgewertet werden.

Für Prüfungszwecke können die Logdateien auch

Log

Save

Format Auswahl

Event-Log-Format

Text-Datei-Format

Komma-Delimited-Format

auf dem prüfereigenen Computer heruntergeladen und dort, z.b. mit Hilfe von Prüfsoftware ausgewertet werden.

Security-Log

System-Log

Application-Log

Überwachung von Domänen

Überwachung von Verzeichnissen/Dateien

Überwachung von Druckaufträgen

Event-Viewer

Übungsaufgabe:

1) Laden Sie die Security-Log-Datei im ASCII-Delimited-Format auf Ihren Personalcomputer.

2) Übernehmen Sie die Datei in Ihr Datenbank- oder Kalkulationsprogramm und beantworten Sie folgende Fragen:

   Anzahl von Logon/Logoff-Prozessen eines bestimmten Anwenders?

   Zugriff auf das System an ungewöhnlichen Tagen und zu ungewöhnlichen Uhrzeiten?

   Haben ausschließlich Firmenangehörige auf das Netzwerk zugegriffen?

Notizen:

2.5 Das Einrichten und Verwalten von Domänen unter WINDOWS-NT

2.5.1 Grundsätzliche Hinweise zur Domänenverwaltung

Das Einrichten und Verwalten von Domänen ist für den Prüfer insoweit interessant, als damit

- Benutzer eingerichtet und geändert werden,
- den Benutzern Logon-Scripts zugewiesen werden können,
- **spezielle Sicherheits- und Schutzeinstellungen** für einzelne Benutzer, Benutzergruppen bzw. für die Überwachung von Domänen an dieser Stelle erfolgen.

Zur Änderung der Sicherheits- und Überwachungseinstellungen bedarf es **umfassender Administratorrechte** innerhalb von WINDOWS-NT. Der **Benutzermanager** läuft standardmäßig auf einem WINDOWS-NT-Server und kann dort als **Programm "USRMGR.EXE"** aus dem Verzeichnis %SystemRot%\System32 aufgerufen werden.

Da für jede WINDOWS-NT-Workstation eine stationäre Benutzerverwaltung vorgenommen werden kann, befindet sich dort ebenfalls ein Benutzermanager, der jedoch ausschließlich für die Verwaltung dieser Workstation einzusetzen ist.

Nach Aufruf des Benutzermanagers wird in einem sich öffnenden Menü **am oberen Bildschirmrand der Domänen-Name** (Usermanager-Domänenbezeichnung) eingeblendet. In dem darunter befindlichen geteilten Bildschirm werden die einzelnen **Benutzer und Benutzergruppen der ausgewählten Domäne** angezeigt.

2.5.2 Sicherheitsoptionen beim Einrichten neuer Anwender

Das Einrichten neuer Anwender erfolgt **innerhalb des Benutzermanagers** für Domänen nach Auswahl der jeweiligen Domäne über die Menüfolge

USER

New User

Beim Einrichten eines neuen Anwenders sollte darauf geachtet werden, daß immer **eindeutige**, auf den jeweiligen Anwender hindeutende Nutzerkennungen und **keine Gruppenbezeichnungen** angewendet werden. Darüber hinaus sollten die optional auszufüllenden Felder FULLNAME und DESCRIPTION, die die Anwenderkurzbezeichnung näher erläutern und Beschreibungen zur Organisationseinheit bzw. Aufgaben beinhalten, ausgefüllt werden.

Mit der Einrichtung eines neuen Anwenders stehen darüber hinaus nachfolgende Optionen zur Verfügung:

- **User must change Password at next Logon**

  Diese Option sollte aktiviert sein, damit der Anwender nach der erstmaligen Anwendung gezwungen ist, das Standard-Eingangspasswort zu ändern.

- **User cannot change Password**

  Passwortänderungen können bei Aktivierung dieser Option nur durch den Systemadministrator erfolgen. Dies sollte nur in begründeten Ausnahmen aktiviert sein.

- **Password never expires**

  Diese Option sollte **nur für solche Benutzer/Objekte** verwendet werden, die für **regelmäßige administrative Arbeiten**, z.B. das **automatische Backup** aus WINDOWS-NT heraus aktiviert werden.

- **Account disabled**

  Durch Aktivierung dieser Option wird ein Nutzer gesperrt. Hierzu ist zu bemerken, daß inaktive oder nicht benötigte Nutzer grundsätzlich aus dem Netzwerk gelöscht werden sollten. Eine Sperrung macht nur dann Sinn, wenn die speziellen Einstellungen dieses Nutzers als Vorlage (sogenanntes **User-Template**) für die Einrichtung neuer Benutzerkennungen verwendet werden soll.

Weitere Optionen, die durch **Druckknöpfe am unteren Bildschirmrand** ausgewählt werden können:

- **Groups**
  Zuweisung eines Benutzer zu einer **Gruppe** mit bestimmten Zugriffsrechten

- **Profile**
  Zuweisung spezieller **nutzerspezifischer Parameter**, wie die Bezeichnung des zu vewendenden Log-Scripts sowie des Home-Verzeichnisses.

- **Hours**
  Festlegung eines **Zeitrahmens**, innerhalb dessen der Nutzer auf dem Serverlaufwerk arbeiten kann.

- **Logon to**
  Explizite **Festlegung der Workstation**, von der aus sich der Benutzer auf dem Serverlaufwerk anmelden kann.

- **Account**
  An dieser Stelle kann für einen Nutzer ein **festes Ablaufdatum** eingetragen werden, nach dessen Ablauf er automatisch gesperrt wird.

- **Dialin**
  Falls beabsichtigt ist, daß der Benutzer von außen über Telefondienste (RAS) auf das Netzwerk zugreifen soll, dann muß die entsprechende Option an dieser Stelle in seinem Benutzerstamm aktiviert werden. Für den Prüfer interessant ist die sogenannte CALL BACK Option, bei der das System nach einer Anmeldung entweder über eine **festdefinierte Rufnummer (Present to)** oder über eine vom Anrufer **frei zu vergebende Telefonnummer (Set by caller)** eingetragen wird.

Bereits an dieser Stelle können mit der **Einrichtung eines neuen Nutzers eine Vielzahl von Sicherheitsoptionen** berücksichtigt werden. Für die Einrichtung neuer Nutzer sollte deshalb ein **schriftliches und prüfbares Konzept** vorhanden sein. Die EDV-Revision sollte sich in Stichproben davon überzeugen, daß die Vorgaben eines solchen Konzeptes bei der Einrichtung neuer Anwender in einem Netzwerk berücksichtigt werden.

2.5.3 Standardsicherheitseinstellungen für Domänen

Zur Absicherung der Server vor unberechtigtem Zugriff einzelner Nutzer gibt es eine Reihe von Standardeinstellungen, die - einmal vorgenommen - für alle einer Domäne zugeordneten Nutzer/Objekte Gültigkeit haben. Die entsprechenden Eintragungen können nach Aufruf des Benutzermanagers mit

POLICIES

Account

eingetragen werden. Nachfolgend sind die einzelnen Parameter mit Vorschlagswerten aufgeführt:

Prameter	Bedeutung	Empfohlene Einstellung
Maximum Password AGE	Verfallzeit des Passwortes	90 Tage
Minimum Password AGE	Minimale Gültigkeitsdauer des Passwortes	Keine (Immediately)
Minimum Password Length	Mindestlänge des Passwortes	6 Stellen
Password Uniqueness	Anzahl der letztgenannten Passwörter, die das System von der Verwendung ausschließt	13 Passwörter
Account Lockout bad logon attemtps	Anzahl von Passwort-Falscheingaben bis zur Sperrung	5 Fehlangaben
Account Lockout Reset count after ... minutes	Überwachungszeitraum für Passwort-Falscheingaben	20 Minuten
Lockout Duration	Sperrzeit nach Passowort-Falscheingaben	Endgültig (Administrator-Freigabe)
Forcibly disconnect remote user from server when logon hours expire	Zwangsabbruch der Netzwerk-Verbindung, wenn die für den Nutzer vorgegebene Nutzungszeit überschritten ist	Aktiviert
Users must log on to change password	Passwortänderung nur bei Arbeit am Server (problematisch bei abgelaufenem Paßwort)	Nicht aktiviert

2.5.4 Die Rechteverwaltung von WINDOWS-NT

2.5.4.1 Grundsätzliches zur Rechteverwaltung

Die **Bewegungsmöglichkeiten** innerhalb eines WINDOWS-NT-Netzwerkes können **in zwei Richtungen begrenzt** werden. Zunächst stehen dort die Objekte, wie z.B. die **Anwender, die aktiv tätig werden und Aktionen** durchführen möchten. Es ist möglich, diesen Aktionsspielraum einzugrenzen. Demgegenüber stehen die **Objekte/Ressourcen, auf die sich solche Aktionen beziehen** und die dementsprechend auch geschützt werden können. Ständig treffen beide Ebenen aufeinander, z.B. das Recht eines Anwenders, Programme innerhalb des Netzwerkes zu starten und demgegenüber den Ressourcenschutz für dieses Programm. I.d.R. haben die **individuellen Benutzerrechte Priorität gegenüber dem jeweiligen Ressourcenschutz**.

Damit die Berechtigungsverwaltung nicht auf der Grundlage der Zuordnung vielfältiger Einzelrechte für einen einzelnen Anwender (aufwendige Administration) erfolgen muß, gibt es eine hierarchische Beziehung:

Domäne

↓

Gruppe

↓

Benutzer

Rechte können auf allen aufgeführten Ebenen vergeben werden und **gelten dann auch jeweils für die untergeordnete Ebene**. Werden z.B. Rechte an eine bestimmte Gruppe vergeben und der Nutzer dieser Gruppe zugeordnet, so verfügt er automatisch über alle Rechte dieser Gruppe. Zusätzlich können jedem **Nutzer** noch **individuelle, über die Gruppenrechte hinausgehende Rechte** zugeordnet werden.

Innerhalb von WINDOWS-NT wird mit der Auslieferung und Installation ein **Standard** zur Verfügung gestellt. Dieser betrifft **angelegte Gruppen**, wie z.B.

- Administrators,
- Account Operators,
- Backup Operators,
- Domain Admins,
- Domain Guests,
- Domain Users,
- Everyone, etc.

und **die diesen Gruppen zugeordneten** Rechte. Da dieser Standard auf allen WINDOWS-NT-Systemen vergleichbar implementiert ist, sollte er aus Revisionsgründen nicht geändert werden. Sind zwingend **Änderungen** notwendig, so dürfen diese **ausschließlich in einem vorher festgelegte, nachvollziehbaren und dokumentierten Verfahren** erfolgen.

Der **Inhalt** der mit bestimmten Aktionen verbundenen **Rechte** wird innerhalb von WINDOWS-NT **nicht verändert**, vielmehr werden diese bereits **vordefinierten Rechte den Gruppen oder Einzelnutzern zugeordnet**. Bei den zuordnungsfähigen Rechten unterscheidet WINDOWS-NT sogenannte Standardbenutzerrechte und erweiterte Benutzerrechte.

2.5.4.2 Einzelheiten zur Berechtigungsvergabe

Die Zuordnung von Benutzerrechten erfolgt innerhalb des **Benutzermanagers** über die Menüfolge

POLICIES

USERRIGHTS

In dem sich öffnenden Fenster können die **Einzelrechte** (Auswahl in dem Fenster Right) zunächst ausgewählt werden, um sie anschließend, **nach Markierung einer Gruppe** bzw. eines einzelnen Nutzers **hinzuzufügen** bzw. zu entfernen.

Nachstehend werden einige wichtige Rechte und deren Standardzuordnung kurz erläutert:

Recht	Bedeutung	Zuordnung
Access this computer from Network	Erstellung einer Verbindung zu dem Rechner	Everyone Administrators
Backup files and directorys	Sicherungsvorgänge	Administrator Backup Operators
Force Shut down from Remote System	Kontrolliertes Abschalten eines Remote-Computers *(überlagert den Schutz von Ressourcen)*	Administrators Server Operaters
Logon Localy	Ermöglicht lokale Anmeldung an der "Server"-Station *(aus Sicherheitsgründen nur für ausgewählte Benutzerkennungen)*	Administrators Account Operators Backup Operators Print Operators Server Operators
Manage Auditing and Security Log	Administration des Überwachungs- und Protokollierungssystems *(Beeinflussung aller entsprechenden Einstellungen)*	Administrators
Take ownership of files or other objects	Veränderung der Eigentümerschaft an Dateien und Verzeichnissen *(überlagert den speziellen Ressourcenschutz)*	Administrators

Erweiterte Rechte		
Recht	**Bedeutung**	**Zuordnung**
Act as part of the operating system	Zugriff auf abgesicherte Betriebssystemteile	Keine Person oder Gruppe
bypass traverse checking	Wechsel von Verzeichnissen innerhalb eines Verzeichnisbaums	Everyone
Generate security audits	Erzeugung von Einträgen im Eventlog	Keiner Person oder Gruppe
Replace a process level token	Ersatz oder Veränderung des nutzerspezifischen Zugriffs- und Sicherheitskennzeichens für Aktionen *(dieses Recht sollte dem System vorbehalten bleiben, da eine Manipulation das gesamte Zugriffsystem außer Kraft setzt)*	Keiner Person oder Gruppe

2.5.5 Kritische Nutzer in einem WINDOWS-NT-System

Kritisch in einem WINDOWS-NT-Netzwerk sind generell **alle Nutzer**, bei denen durch **exzessive Rechtevergabe Funktionstrennung und das Vier-Augen-Prinzip nicht berücksichtigt werden**. Es sind darüber hinaus Nutzer, die ohne konkrete Aufgabe in das System eindringen und ggf. Daten ausspähen können.

Der vorstehenden Definition entsprechend, können bei einer **ungeplanten, mit der Zeit reifenden Netzwerkorganisation, ohne ausreichende Netzwerkrichtlinien und Vorgaben eine große Anzahl kritischer Nutzerkennungen** vorhanden sein, auf die an dieser Stelle nicht eingegangen werden kann. Die nachfolgenden Ausführungen beschränken sich vielmehr auf solche Nutzerkennungen, die standardmäßig als kritisch anzusehen sind.

❑ **Nutzerkennung Guest**

Die Nutzerkennung Guest wird seitens des WINDOWS-NT-Systems standardmäßig mit der Installation eingerichtet. Sie dient dazu, auch dann einen Zugang in das System zu ermöglichen, wenn ein Benutzer nicht angelegt ist, oder sich mit falschem Paßwort anmeldet.

Standardmäßig ist die **Benutzerkennung Guest ohne Paßwort** angelegt und innerhalb des Systems deaktiviert, so daß keine unberechtigten Eindringversuche erfolgen können. Ist er aktiviert, so ist es grundsätzlich nicht unmöglich, Zugriffe auf das System und auf den Server zu erlangen.

Der **Revisor** sollte sich im Rahmen seiner Prüfung davon überzeugen, daß der **Guest Account** ausschließlich über **sehr beschränkte Berechtigungen** verfügt, bzw. innerhalb des Systems gesperrt ist.

❏ **Administrator**

Als Administrator ist man mit umfassenden Rechten auf jedem WINDOWS-NT-System eingerichtet. Für den Administrator sollten unter Revisionsgesichtspunkten eine Reihe von Regelungen eingehalten werden.

- **Administratorkennung nur für Administratoraufgaben**

  Ein Netzwerkadministrator sollte sich **nur dann mit seiner Administratorkennung** an dem Netzwerksystem anmelden, **wenn er tatsächlich hierzu notwendige Arbeiten** durchführt. Bereits das Gruppieren einer z.B. virenbefallenen Datei könnte aufgrund der ihm zugeordneten umfassenden Rechte zu schwerwiegenden Störungen der Integrität innerhalb des Systems führen. Für alltägliche Arbeiten sollte er deshalb über eine **zusätzliche Benutzerkennung mit eingeschränkten Berechtigungen** verfügen und diese verwenden.

- **Neubezeichnung des Administrators**

  Da der Administrator mit seiner Kennung auf jedem WINDOWS-NT-System standardmäßig eingerichtet wird, handelt es sich um einen Nutzer mit niedrigem Sicherheitslevel. Die **Originalbezeichnung ADMIN** sollte deshalb in der produktiven Netzwerkumgebung **umbenannt werden**. Darüber hinaus sollte der Administrator an sein eigenes **Paßwort strenge Richtlinien** anlegen als der normale User. Auf keinen Fall darf es Dritten bekannt werden.

- **Beschränkung der Administratorfunktion auf lokales Netzwerk**

  Da die Administratorfunktion mit vielfältigen Gefahren verbunden ist, sollte der entsprechenden Benutzerkennung **keine Möglichkeit** zugeordnet werden, von außen **über RAS auf das System zuzugreifen**. Die entsprechende Möglichkeit kann, wie bereits erläutert, innerhalb des User-Accounts deaktiviert werden.

❏ **Kritische Benutzergruppen**

Die Zuordnung von Rechten innerhalb eines WINDOWS-NT-Netzwerkes erfolgt i.d.R. gruppenorientiert, wobei für bestimmte feststehende Aufgaben bereits eine Reihe von **Standardgruppen** vorgegeben sind. Die über diese Gruppen vorzufindenden Rechte und Möglichkeiten sind äußerst vielfältig und divergieren, je nach dem ob man eine lokale Arbeitsstation bzw. einen Server in einem WINDOWS-NT-Netzwerk betrachtet.

Auf den folgenden Seiten findet sich jeweils eine kurze schematische Darstellung.

	Standardgruppen							
Möglichkeiten	**Admin**	**Server Operator**	**Account Operator**	**Backup Operator**	**Print Operator**	**User**	**Everyone**	**Guest**
Anmeldung auf diesen Rechner vom Netz	X						X	
Lokale Anmeldung am Server	X	X	X	X	X			
Eigentümerschaft von Dateien ändern	X							
Sicherheitsprotokollierung beeinflussen	X							
Rechner herunterfahren	X	X	X	X	X			
Backup-Funktionen	X	X		X				
Entfernte Rechner herunterfahren	X							
Recovering Funktionen	X	X		X				
Arbeitsstationen an Domänen anmelden	X							
Gerätetreiber entfernen und laden	X							
Gruppen administrieren	X		X					
Benutzer einrichten	X		X					
Benutzerrechte ändern	X		X					
System-Monitoring und Überwachung	X							
Platte formatieren	X							
Sperre von Netzlaufwerken	X	X		X				
Laufwerkssperren aufheben, nicht berücksichtigen	X	X						
Verzeichnisse freigeben (Share)	X							
Drucker freigeben (Share)	X	X						
Programmgruppen erstellen	X	X						
Profile erstellen/ pflegen	X	X						

Bild 15Standardrechte und Möglichkeiten von Gruppen auf **WINDOWS-NT-SERVERN**

	Standardgruppen							
Möglichkeiten	**Admin**	**Power USER**	**Backup Operator**	**USER**	**Everyone**	**Guest**	**Everyone**	**Guest**
Anmeldung auf diesen Rechner vom Netz	X	X			X			
Lokale Anmeldung am Rechner	X	X	X	X	X	X		
Eigentümerschaft von Dateien ändern	X							
Sicherheitsprotokollierung beeinflussen	X	X						
Rechner herunterfahren	X	X	X	X	X			
Backup-Funktionen	X		X					
Entfernte Rechner herunterfahren	X	X						
Recovering Funktionen	X		X					
Gerätetreiber entfernen und laden	X	X						
Gruppen administrieren	X	X		X				
Benutzer einrichten	X	X						
Benutzerrechte ändern	X							
System-Monitoring und Überwachung	X	X						
Platte formatieren	X							
Sperre von Laufwerken	X	X			X			
Laufwerkssperren nicht berücksichtigen	X	X						
Verzeichnisse freigeben (Share)	X	X						
Drucker freigeben (Share)	X	X						
Programmgruppen erstellen	X	X						
Profile erstellen/ pflegen	X	X	X	X				

Bild 16Standardrechte und Möglichkeiten von Gruppen auf **WINDOWS-NT-WORKSTATIONS**

Eine Reihe der aufgeführten Gruppen verfügt über sehr umfassende Rechte, die durchaus dazu geeignet sind, die Integrität der im Netzwerk verwalteten Daten zu beeinflussen. Der Revisor sollte sich deshalb darüber informieren, welchen Gruppen jeweils eine einzelne Benutzerkennung zugeordnet ist. Zur **Identifizierung der Mitglieder einer bestimmten Gruppe** ist der **Benutzermanager** zu aktivieren. Über die Menüfolge

USER

Select Users

öffnet sich ein neues Fenster, in dem die gewünschten Gruppen markiert werden können. Anschließend können mit dem Befehl **SELECT** alle Anwender markiert werden, die der ausgewählten Gruppe angehören.

2.4.7 Zugriffschutz und Zugriffsmöglichkeiten auf Verzeichnis- und Dateiebene

2.4.7.1 Übersicht über Schutzmechanismen auf Verzeichnis- und Dateiebene

Die Schutzmöglichkeiten auf Verzeichnis- und Dateiebene hängen - wie Eingangs erläutert - vom gewählten Dateisystem ab.

Dateisystem

FAT	**NTFS**
• Zugriffschutz nur auf Verzeichnisebene	• Zugriffschutz auf Verzeichnis und Dateiebene
• Kein Zugriffschutz bei lokalem Zugriff auf die Ressourcen	• Zugriffschutz bei Netz- und lokalem Zugriff
• Bootvorgang mit DOS-Diskette möglich *(Zugriff auf Dateien)*	• Kein Bootvorgang über Diskette

Aus der dargestellten Übersicht ergibt sich, daß die **erweiterten und erwarteten speziellen Sicherheitsmechanismen** von WINDOWS-NT nur zum tragen kommen, **wenn das Dateisystem NTFS** zum Einsatz kommt.

Grundsätzlich kann auf die Ressourcen eines Verzeichnisses bzw. auf das Verzeichnis selbst nur zugegriffen werden, wenn es zuvor für die Arbeit unter WINDOWS-NT freigegeben wurde. Die **Freigabe** erfolgt dadurch, daß für das betreffende Verzeichnis ein sogenanntes "Share" eingerichtet wird. Mit der **Einrichtung eines Shares können hiernach vielfältige Schutzmechanismen**, die nachstehend erklärt werden, aktiviert werden. Die

nachstehende Erläuterung beschränkt sich auf die Darstellung von Sicherheitseinstellungen, die mit einem **Share unter NTFS** verbunden sind.

2.4.7.2 Datei- und Verzeichnisrechte beim Einsatz von NTFS

Die Freigabe von Verzeichnissen, das sogenannte Share erfolgt in folgenden Schritten:

Dateimanager (Explorer) aufrufen

Gewünschtes Verzeichnis markieren

File

Properties

Sharing

Shared S auswählen

An dieser Stelle können die notwendigen Angaben zur Freigabe der Ressourcen erfolgen. Die hier erfolgten Freigaben beziehen sich jedoch ausschließlich auf den lokalen Rechner, an dem gerade gearbeitet wird. Sollen **Freigaben auf anderen Netzwerkrechnern** erfolgen, so benötigt man hierzu einen sogenannten **"Server-Manager"**, den man (sofern installiert) über die Befehlsfolge

Start

Programs

Administrativ Tools

Server Manager

aktiviert.

Nach Markierung und Auswahl der gewünschten Domäne werden **alle dieser Domäne zugeordneten Server und Workstations** angezeigt. Der entsprechende Rechner wird markiert und mit der Befehlsfolge

Computer

Properties

Security

stehen nun alle gewünschten **Optionen zum Einrichten und Verwalten von Shares** (siehe Druckknopf Shares) zur Verfügung.

Außer der Verwaltung von Shares lassen sich an dieser Stelle weitere **Beobachtungen** vornehmen. Es ist ohne weiteres möglich, festzustellen,

- **welche User wie lange und von welchem Rechner auf** dem gewählten Serverlaufwerk tätig sind,
- **welche Ressourcen** zur Zeit auf dem gewünschten Rechner genutzt werden.

Das Anzeigen vorhandener "Shares" erfolgt, in dem man zunächst das entsprechende Verzeichnis markiert und mit der Befehlsfolge

Computer

Shared Directories

Properties

Security

Permission
Auditing
Ownership

auswählt. Für ein Verzeichnis können hiernach differenziert die folgenden Rechte zugeordnet werden

Grundrechte für Verzeichnisse und Dateien	
R-Read-Lesen	Anzeige von Dateinamen, Inhalten, Attributen, Berechtigungen und Eigentümerschaften
W-Write-Schreiben	Verzeichnisse und Dateien erstellen und Attribute ändern
X-Execute-Ausführen	Wechsel und Unterverzeichnisse sowie starten von Programmen
D-Delete-Löschen	Löschen von Verzeichnissen und Dateien
P-Change Permissions	Zugriffsberechtigung für Dateien ändern
O-Take ownership	Wechsel der Eigentümerschaft für Verzeichnisse und Dateien

Aus den vorbezeichneten **Grundrechten** wurden unter speziellen Bezeichnungen innerhalb von WINDOWS-NT **Standardberechtigungen für Verzeichnisse und Dateien** definiert, die in den nachfolgenden Aufstellungen dargestellt sind.

❏ Standardberechtigungen für Verzeichnisse

	No Access Keine	**List** RX	**Read** RX	**Add** WX	**Add and Read** RWX	**Change** RWXD	**Full Control** ALL
Verzeichnisinhalt anzeigen		X	X		X	X	X
Verzeichnisattribute anzeigen		X	X	X	X	X	X
Verzeichnisattribute ändern				X	X	X	X
Unterverzeichnis aufrufen		X	X	X	X	X	X
Eigentümerschaft und Rechte für Verzeichnis anzeigen		X	X	X	X	X	X
Verzeichnis löschen						X	X
Datei oder Unterverzeichnis im Verzeichnis löschen							X
Zugriffsberechtigung für Verzeichnis ändern							X
Eigentümerschaft ändern							X

❏ Standard-Rechte auf Dateiebene

	No Access Keine	**List** RX	**Read** RX	**Add** WX	**Add and Read** RWX	**Change** RWXD	**Full Control** ALL
Dateiinhalt anzeigen			X		X	X	X
Eigentümer und Rechte anzeigen			X		X	X	X
Dateiattribute anzeigen			X		X	X	X
Dateiattribute ändern						X	X
Programm ausführen			X		X	X	X
Dateinihalt ändern						X	X
Datei löschen						X	X
Zugriffsberechtigung ändern							X
Eigentümerschaft ändern							X

Für die Berechtigungsgestaltung in einem WINDOWS-NT-Netzwerk wichtig ist es zu verstehen, daß **für jedes gewünschte Verzeichnis verschiedenste "Shares" mit unteschiedlichen Rechten** angelegt werden können. Die Verbindung zu den **Gruppen bzw. den Nutzern** innerhalb des Netzwerkes erfolgt, in dem man diese **als Berechtigte in das Shared-Verzeichnis aufnimmt**.

Für die Beurteilung der sich an dieser Stelle für den Anwenderergebenden Rechte ist der Zugriffsmechanismus von Bedeutung, der nachfolgend dargestellt ist.

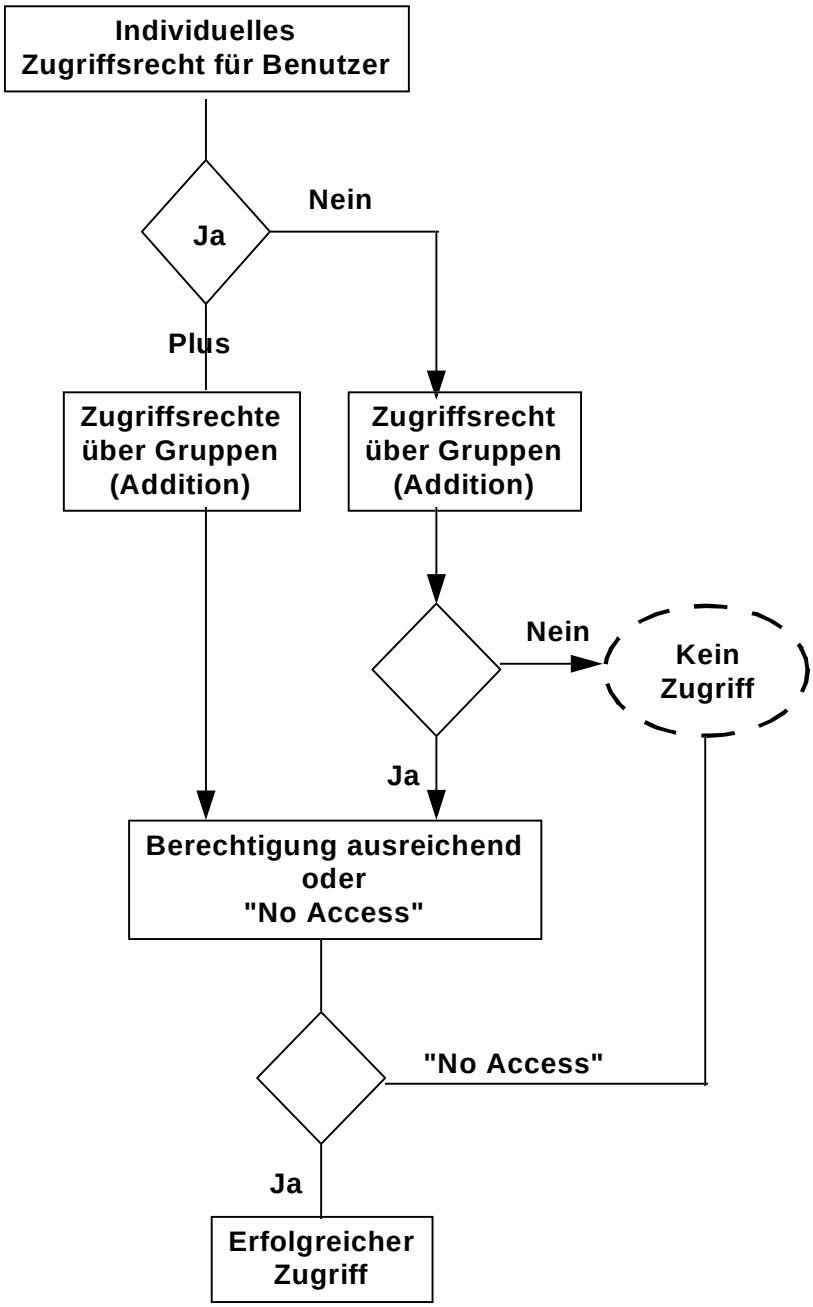

Bild 17 Zugriffsmechanismus für Benutzer

Fragen und Übungen:

1) Erläutern Sie die grundlegenden Mechanismen der Rechtevergabe in einem WINDOWS-NT-Serversystem?

2) Erklären Sie die Addition von Rechten in einem Netzwerksystem?

3) Welchen Effekt hat die Zuweisung eines Netzes bzw. seiner Gruppe zu einem "Share" mit der Eintragung "No Access"?

4) Erläutern Sie den Unterschied von Grundrechten für Datei und Verzeichnisse und Standardberechctigungen auf Datei- und Verzeichnisebene?

5) Welche Standardgruppen finden wir u.a. in einem WINDOWS-NT-Netzwerk?

6) Was sind die Nachteile von FAT gegenüber NTFS?

Notizen:

Aus der vorgenannten Abbildung ergibt sich, daß sich grundsätzlich die **Einzel- und die Gruppenrechte addieren, vorausgesetzt die Arbeit mit einem gewünschten Objekt wird nicht** von irgend einer Stelle **durch "No Access"** unterbrochen. In einem solchen Fall ist definitif keinerlei Zugriff mehr möglich. Dies gilt auch, wenn man grundsätzlich die Erlaubnis zum Zugriff und für die Arbeit mit einer Datei hat, jedoch der **Weg zu dieser Datei** über die verschiedenen **Verzeichnisse** an irgendeiner Stelle **durch ein "No Access" auf Verzeichnisebene unterbrochen wird**.

Zuletzt sei an dieser Stelle auf einen noch für den EDV-Revisor interessanten Umstand hingewiesen, daß mit der **Einrichtung von "Share und NTFS"** auch die **Überwachung (Audit)** der ausgewählten Objekte aktiviert bzw. deaktiviert werden kann.

2.4.8 Weitere Prüfungshandlungen

2.4.8.1 Systemeinstellungen zur Datensicherheit

Im Hinblick auf die Sicherheit der in einem Netzwerk verwalteten Daten ist es notwendig, zu prüfen, ob die **Daten regelmäßig gesichert** werden und die **Unterbringung der Sicherungsbänder** den hierzu notwendigen Regelungen innerhalb eines Unternehmens entspricht.

Im täglichen Betrieb muß darüber hinaus sichergestellt sein, daß **System- und Plattenfehler nicht zu einem** unwiderruflichen Datenverlust oder zu einem **längeren Systemausfall** führen. Die hierzu geeigneten Mechanismen reichen von der Datenspiegelung bis zur **RAID5-Technik**, die beide von WINDOWS-NT unterstützt werden. Da die letztere Technik einen Austausch defekter Laufwerke auch bei laufendem Betrieb ermöglicht, sollte sie in zeitkritischen Systemen bevorzugt werden, auch wenn hierzu aufwändige RAID-Controler eingesetzt werden müssen. Die Administration bedient sich für die hierzu notwendigen Einstellungen eines **speziellen Tools, des "Disk Administrators"**. Dieser sollte jedoch - aufgrund der vielfältigen Möglichkeiten Daten zu beeinflussen - für Prüfungszwecke nicht eingesetzt werden.

Eine **grundsätzliche Übersicht** über die zu einem **Netzwerk gehörenden Einstellungen** kann der EDV-Revisor darüber hinaus in Zusammenarbeit mit dem zuständigen Administrator erhalten, wenn er das Diagnosewerkzeug von WINDOWS-NT durch Zugriff auf die Gruppe

Administrativ

Tools

aktiviert.

Notizen:

2.4.9 Werkzeuge für die Prüfung in einer WINDOWS-NT-Umgebung

Die Prüfung in einer WINDOWS-NT-Umgebung ist außerordentlich aufwendig. Um sie in einem vertretbaren Zeitrahmen durchführen zu können, empfiehlt es sich, geeignete Werkzeuge einzusetzen. Hierzu seien nachstehend zwei Beispiele aufgeführt:

❑ **Programme aus dem MS-Ressource-Kit**

Es handelt sich um eine **Ansammlung von Programmen**, die normalerweise **für Administrationszwecke** eingesetzt werden und die zusätzlich zu dem Betriebssystem erworben werden können. Einige der innerhalb des Ressourcekit vorhandenen Programme können jedoch sehr gut für Prüfungszwecke verwendet werden.

- **FINDGRP.EXE**
  Suche aller Benutzer einer Gruppe
- **ADDUSERS.EXE**
  Übernahme der Informationen zu Benutzerkennungen in eine Datei
- **PRMS.EXE**
  Darstellung der Zugriffsrechte, die Nutzer für Dateien haben
- **DOMMOM.EXE**
  Übersicht über die Netzwerkorganisation, Domänen und Vertrauensstellungen
- **AUDITKIT.HLP**
  Detaillierte Erläuterungen zu den Audit-Kategorien des EVENT VIEWER

Ein von dritter Stelle erstelltes Programm, welches Sicherheit und Zugriffschutz einer WINDOWS-NT-Netzwerkumgebung in kürzester Zeit analysiert und alle sicherheitsrelevanten Informationen, den Sicherheitsstatus sowie Sicherheitslücken in übersichtlichen Grafiken und Detailbildschirmen darstellt, ist der **Kane Security Analyst**.

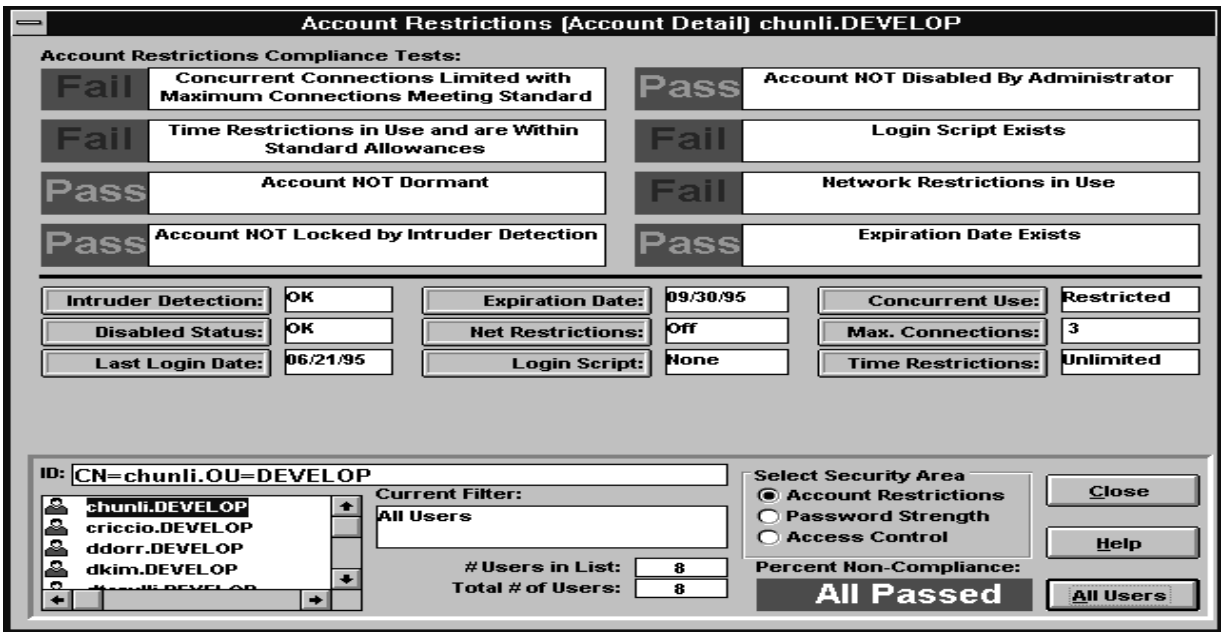

Bild 18 Analyse von WINDOWS-NT-Servern mit Hilfe von "KSA"

Die für die Revision interessanteste Funktion dürfte der **umfassende, vollständig aufbereitende Prüfungsbericht** sein, den dieses Programm automatisch generiert.

2.5 Analyse von Netware/Novell-Umgebungen

NetWare verfügt mit der Version 4.x über ein Betriebssystem mit den derzeit wohl ausgefeiltesten Sicherheitsmechanismen sowie mit umfangreichen Absicherungs- und Protokollierungsmöglichkeiten, die seitens der EDV-Revision ausgewertet werden können. Die Zusammenstellung aller Daten und die Beurteilung des Sicherheitsstandards ist allerdings in dieser Umgebung mit erheblichem zeitlichem Aufwand verbunden. Ein Leitfaden zur Prüfung grundsätzlicher Sicherheitseinstellungen findet sich als Anlage.

Für eine schnelle und umfassende Analyse wird auch in diesem Fall der Einsatz zweckgerichteter Programme empfohlen. Die bereits angesprochene Software Kane Security Analyst wird ebenfalls für diese Plattform angeboten.

2.6 Analyse auf weiteren Betriebssystemen

Neben den aufgeführten EDV-Plattformen finden sich weitverbreitete Maschinen, wie z.B. die **IBM AS/400** sowie **DEC/VAX unter VMS**.

Zur Unterstützung der EDV-Revision stehen auch für diese EDV-Umgebungen entsprechende **Analysetools** zur Verfügung, wie z.B.:

- PC-DEC-Audit, Trillion Software, UK,
- Audit Master (IBM AS/400), Rapport, UK,
- Security Detective (DEC und AS/400), D.A.T.A. Services, UK,

die eine schnelle und effiziente Erfassung aller Sicherheitseinrichtungen ermöglichen.

Eine **systemübergreifende revisionsspezifische Analyse**, die sowohl die Großrechner als auch unterschiedliche Midrange- und Netzwerkumgebungen einbezieht, soll mit dem Produkt **CONSUL/Enterprise Audit** ermöglicht werden.

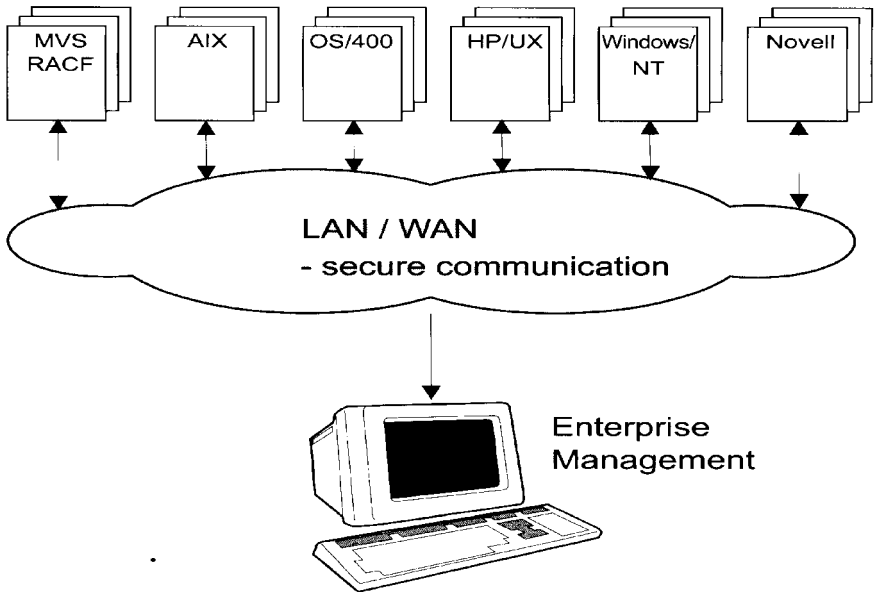

Bild 19 Sicherheitsanalyse in einer heterogenen EDV-Umgebung mit Hilfe von "CEA"

2.7 Weitere Analysen zum Systembetrieb

Selbst die beste EDV-Administration kann **Systemausfälle durch Betriebssystemfehler, defekte Speichermedien oder eine Stromunterbrechung nicht vollständig ausschließen**. Je nach Art des Defektes besteht grundsätzlich die Gefahr schiefer Datenbestände, fehlerhafter **Datensatzverkettungen bzw. eines vollständigen Verlustes aller auf einem Serverlaufwerk befindlichen Dateien**. Technische Optionen, wie etwa unterbrechungsfreie Stromversorgung oder Systemzurücksetzung eines unvollständig abgebrochenen Datenbankupdates erhöhen zwar die Datensicherheit, können jedoch keine **revisionsfreundliche Ausgestaltung der Datensicherung** ersetzen.

An die **Datensicherung** in einer Client-/Server-Umgebung sind die gleichen, strengen Kriterien anzulegen, wie sie vordem auf Großrechnerebene üblich waren. Dazu gehören verbindliche Regelungen für Tages- und Wochensicherung von Daten und Programmen, automatische Sicherungsläufe für Serverlaufwerke und Anwendungsstationen und nicht zuletzt das eindeutige Beschriften und die sichere Aufbewahrung der Sicherungsbänder.

Die Revision sollte sich von der Wirksamkeit dieser Vorgaben im Rahmen **simulierter Katastrophenübungen** überzeugen und sich die Rekonstruktion gesicherter Datenbeständen von Zeit zu Zeit vorführen lassen.

3 Dokumentation und Prüfung der mit der EDV-Anwendung verbundenen baulichen und organisatorischen Gegebenheiten

Mit der Individualisierung von Computeranlagen und dem einhergehenden Preisverfall **reduziert** sich sowohl bei den Anwendern als auch - gefährlicher - bei der Systemadministration erkennbar das **Gefühl für die Bedeutung der EDV-Anwendung im Unternehmen**.

Während ein Großrechner entsprechend seiner Größe und seinem Wert in hermetisch abgesicherten Räumlichkeiten untergebracht wurde, findet sich ein vergleichbar leistungsfähiger (kleiner) **UNIX-Server ungeschützt mitten in Großraumbüros unter den Schreibtischen der Netzwerkadministratoren**. Eine gefährliche Entwicklung: das Gefahrenpotential hat durch die Miniaturisierung der EDV-Komponenten eher zu- als abgenommen. So paßt eine Mehr-Gigabyte-Festplatte mit wesentlichen Daten eines Unternehmens **problemlos in die Westentasche** und ist - wartungsfreundlich - ebenso schnell ausgebaut wie entwendet.

Bereits bei der Einrichtung eines Netzwerkes sollte die Revision durch ihre Begleitung sicherstellen, daß die Serverlaufwerke in einem räumlich abgetrennten, gegen unbefugten Zugang, Diebstahl und Brand abgesicherten Teil des Unternehmens untergebracht werden.

Revisionsfreundlich ist der EDV-Betrieb in einer Netzwerkumgebung darüber hinaus, wenn die **Verantwortlichkeiten für den laufenden Systembetrieb** geregelt sind.

Dazu gehört eine eindeutige **Abgrenzung der Tätigkeitsbereiche** von

- Netzwerkadministratoren,
- Netzwerk-Supervisoren,
- Datenbankadministratoren,
- Organisations- und Anwendungsprogrammierer,
- verantwortlichen Spezialisten für die Administration und die Berechtigungsvergabe beim Einsatz komplexer Applikationen.

Die oft in **mittelständischen Unternehmen anzutreffende Funktionshäufung** in Client-/ Serverinstallationen erhöht das Gefahrenpotential für den EDV-Betrieb erheblich.

Wichtig ist auch die Entwicklung und Umsetzung **klar definierter Berechtigungskonzepte** sowohl

- auf Betriebssystemebene,
- auf Datenbankebene und
- auf Applikationsebene,

die gemeinsam mit der Revision und **vor produktiver Inbetriebnahme der EDV-Anwendung** erfolgen sollte.

Die **Berechtigungsvergabe** auf allen aufgezeigten Ebenen ist **personen-, aufgaben- und gruppenorientiert**, äußerst **komplex und schwer prüfbar**. Die einzelnen Anwender können sehr flexible **Lese- und Schreibrechte** für bestimmte **Handlungen, Transaktionen, Tabellen, Dateien oder Datenverzeichnisse** eingeräumt werden. Die **Anzahl der Anmeldungen** bei Eingabe eines **falschen Paßwortes** ist ebenso begrenzbar, wie der **Zeitraum**, innerhalb dessen ein Anwender im Netzwerk arbeiten kann.

Weitere Optionen verlangen Paßwortänderungen nach einer bestimmten Zeit und schließen Paßwörter mit unbestimmtem Inhalt oder unzureichender Länge aus. An dieser Stelle hat die EDV-Revision durch ihre **Vorgaben zur Gestaltung des Berechtigungskonzeptes sowie zur Zugriffssicherung** vielfältige Möglichkeiten Gefahren auszuschließen.

Betriebs- und Datenbanksysteme sowie die Anwendungsprogramme bieten i.d.R. Übersichten der eingerichteten Zugriffsberechtigungen. Jedoch erhält der EDV-Revisor auch hier keine auf seine speziellen Bedürfnisse ausgerichtete Zusammenstellung der Daten.

Für diesen sehr zentralen Punkt der EDV-Revision kann der **Einsatz bereits bezeichneter Zusatzprogramme** empfohlen werden, die - je nach Einsatzbereich - weitgehend automatisch Zugriffsberechtigungen einschließlich aller Restriktionen personenbezogen und thematisch geordnet erfassen.

4 Arbeitspapiere und Berichte

Neben der produktiven Arbeit innerhalb der Systeme beeinflussen zwei weitere Faktoren,

- die Erstellung des **Arbeitsprogramms** und
- die **Prüfungsberichtserstellung**,

die Effizienz der EDV-Revision.

Die für die Erstellung eines **Prüfprogramms** sinnvollen **Fragebögen** können **manuell geführt werden**.

Sinnvoller ist eine PC-geführte Anwendung, bei der ein individuelles Prüfprogramm aus vorhandenen Fragebögen entwickelt, Fragen beantwortet und ein Bericht erstellt werden kann. Der Nutzen einer solchen Anwendung hängt dabei wesentlich von **Umfang und Qualität der integrierten** Fragebögen ab.

Zwei Systeme

- **QRS, IBO, D**
- **REDIS, IIT GmbH, D,**

  welche für die Unterstützung von Projekten der Internen Revision entwikkelt wurden, verfügen aufgrund ihrer Herkunft aus einem Dienstleistungsrechenzentrum für Banken, über **detaillierte Fragenkataloge zu den Themen Datenschutz und -sicherheit**.

Speziell für die **EDV-Systemprüfung** entwickelt wurden die Programme:

- **DELOS**

  Eine Programmierung der DATEV, die mit Hilfe integrierter Checklisten und zusätzlicher Erläuterungen nach einer Prüfung einen Rohbericht liefert. Das Programm steht nur Mitgliedern der DATEV zur Verfügung.

- **COP-IT, Code of practice for information security management**

  Ein Standardwerk zur Prüfung der Informationstechnologie mit integrierten Fragebögen, Erläuterungen und Rohbericht. Die Fragebögen lehnen sich an den **angelsächsischen Standard**, der in einigen Bereichen, besonders zu dem Punkt Ordnungsmäßigkeit, von der deutschen Sicht abweicht, an. Für international tätige Unternehmen handelt es sich um ein gutes Hilfsmittel.

- **FAMA-PC, IDW-Verlag GmbH, D**

  Es handelt sich um ein **WINDOWS-System zur Unterstützung der EDV-Systemprüfung**. Integriert ist der durch den Fachausschuß für moderne Abrechnungssysteme **(FAMA)** entwickelte **Fragebogen**, der sich stark an die Anforderungen der Wirtschaftsprüfung anlehnt und Fragen der Ordnungsmäßigkeit in den Vordergrund stellt. Das Programm unterstützt die Prüfung mit Checklisten, liefert eine grafische Übersicht über den Sicherheitsstandard eines Systems und einen Rohbericht nach Abschluß der Prüfung. Es ist an vielen Stellen konfigurierbar, kann mit neuen Fragenkatalogen, Einzelfragen und Gewichtungen sowie Erläuterungen zu den Fragen ergänzt werden.

III Zusammenfassung

Datenschutz und -sicherheit sowie die Ordnungsmäßigkeit der Datenverarbeitung sind in weitgehend offenen, modular aufgebauten und dezentral betriebenen Client-/Server-Umgebungen zunehmend schwierig zu realisieren. Diese Schwierigkeit verlangt z**usätzliche Kontrollen durch die EDV-Revision**. Sie sollte deshalb auf eine revisionsfreundliche Gestaltung der EDV-Umgebung Einfluß nehmen. Dazu zählen u.a.:

- ❏ eine aktuelle Dokumentation der verwendeten Hardware in Dateiform,
- ❏ eine aktuelle Dokumentation zugelassener und lizensierter Anwendungsprogramme in Dateiform,
- ❏ die Zwangsprotokollierung aller revisionsrelevanten Vorgänge sowohl auf Betriebsystem- als auch auf Datenbankapplikationsebene mit Erläuterung zu Auswirkungen und Bedeutung einzelner Fehlertypen,
- ❏ ein nachprüfbares Konzept für die Sicherung von Daten der Server- und Arbeitsplatzrechner,
- ❏ eine abgesicherte Unterbringung der Serverlaufwerke und
- ❏ ein abgestimmtes Konzept für die Zugriffsberechtigungen auf allen EDV-Schichten.

Speziell für die Revision entwickelte Hilfsprogramme erhöhen die Effizienz der Prüfung, verbessern den Sicherheitsstatus der EDV und reduzieren die damit verbundenen Gefahren.

Anhang A

Prüfungshandlungen in Netzwerkumgebungen bei Verwendung verschiedener Betriebssysteme

A. Prüfungshandlungen bei Verwendung von WINDOWS-NT-Netzwerk

1. Grundsätzliche Einstellungen zur Nutzer- und Gruppenverwaltung

❏ Wird eine **eindeutige User-ID** verlangt? User-Manager

❏ Haben **nur zugelassene User** Zugriff auf das System und ist der Guest-Account gesperrt?

User-Manager

❏ Wird für alle User-ID's eine individuelle und keine Gruppenkennung verwendet?

❏ Gibt es keine User-ID's ohne Paßwort?

❏ Werden die User-ID's von mehr als drei Monaten nicht im Netz tätigen Anwender gelöscht?

❏ Haben ausschließlich hierzu autorisierte Administratoren Zugriff auf Dateien, die sich auf Sysytemebene befinden?

❏ Sind ausführbare Programme innerhalb des Netzwerkes vor unberechtigten Änderungen und Modifikationen geschützt?

❏ Gibt es ein nachvollziehbares Verfahren für die Einrichtung von Share-Verzeichnissen und die Zuordnung von Gruppen zu diesen Verzeichnissen?

❏ Gibt es ein nachvollziehbares und transparentes Verfahren für das Anlegen von Gruppen, deren Berechtigung und die Zuordnung von Anwendern zu diesen Gruppen?

❏ Wird die Gruppe Everyone nicht exzessiv für die Zuordnung von Anwendern genutzt?

❏ Sind in Gruppen mit priviligierten Rechten, wie z.B. solchen mit Administrator- und Operatorfunktion ausschließlich hierzu bestimmte Nutzer angelegt?

❏ Ist der Zugriff auf das Netzwerk zu ungewöhnlichen Zeiträumen, z.B. Abends und an Wochenenden, eingeschränkt?

Benutzer Manager - New User - Properties

❏ Wird ein Useraccount automatisch abgemeldet, wenn er zu unautorisierten Zeiten innerhalb des Netzwerkes arbeitet?

Account Policy Bildschirm

Prüfungshandlungen in Netzwerkumgebungen bei Verwendung verschiedener Betriebssysteme

A. Prüfungshandlungen bei Verwendung von WINDOWS-NT-Netzwerk

2. Einstellungen zum Paßwort

❏ Ist ein Paßwort für jeden Nutzer notwendig?

Benutzer Manager - New User

❏ Muß das Paßwort bei der erstmaligen Anmeldung geändert werden?

Benutzer Manager - New User

❏ Verfügt das Paßwort über eine ausreichende Anzahl von Stellen?

Account Policy - Minimum Paßwortlänge

❏ Kann das Paßwort über längere Zeit nicht verwendet werden?

Account Policy - Paßwort Unicness

❏ Gibt es ein festes Verfallsdatum für das Paßwort?

Account Policy - Maximum Paßwort Age

❏ Kann ein Paßwort so vom Anwender geändert werden?

Account Policy - Minimum Paßwort Age

❏ Werden fehlerhafte Paßworteingaben aufgezeichnet?

Account Policy - Account Logout

❏ Können gesperrte User-ID's ausschließlich durch den Administrator freigegeben werden?

Acount Policy - Logout Duration

3. Überwachungs- und Protokollierungsfunktionen

❏ Sind die Überwachungs- und Protokollierungsfunktionen aktiviert?

User Manager - Domain Auswahl - Audit these Events

❏ Ist sichergestellt, daß alle systemnahen Aktivitäten aufgezeichnet werden?

Audit Policy
- Security Policy
- Changes/Restart
- Shutdown - System

Prüfungshandlungen in Netzwerkumgebungen bei Verwendung verschiedener Betriebssysteme

A. Prüfungshandlungen bei Verwendung von WINDOWS-NT-Netzwerk

3. Überwachungs- und Protokollierungsfunktionen

❏ Ist sichergestellt, daß alle Aktivitäten über Telefondienste aufgezeichnet werden?

- Parameter in der Registry gesetzt
- PPP.Log und DEVICE.Log auswerten

❏ Ist sichergestellt, daß unautorisierte Zugriffe auf das Netzwerk sowie die Dateien aufgezeichnet werden?

Audit Policy
- Logon on/off
- File and Object
- Use of Userrights
- User and Groupmanagement
- Process Tracking

4. Abschottung des Systems nach außen

❏ Ist sichergestellt, daß kein unberechtigter RAS Zugriff auf das Netzwerk erfolgt?

Benutzermenü - Call back -Present to

❏ Ist sichergestellt, daß Kommunikationsprots ausschließlich für zulässigen Datenverkehr verwendet werden?

Server Manager - Kommunikationsports - Port Status

❏ Ist sichergestellt, daß der Datenverkehr innerhalb des Netzwerkes ausschließlich verschlüsselt läuft?

❏ Ist sichergestellt, daß die Paßwortdateien verschlüsselt gespeichert und restriktiv vor unbefugtem Zugriff geschützt sind?

Prüfungshandlungen in Netzwerkumgebungen bei Verwendung verschiedener Betriebssysteme

B. Prüfungshandlung bei Verwendung von NetWare/Novell 3.x

1. Schutzeinstellungen zur Paßwortverwendung

❏ Wird für den Netzzugang ein Paßwort benötigt?

Programm Syscon

❏ Sind User-ID's vorhanden, die kein Paßwort benötigen?

Programm Bind View

❏ Wird regelmäßig auf fehlende Paßwörter geprüft?

Programm Bind View

❏ Haben alle Paßwörter eine gewünschte Mindestlänge?

Programm Syscon

❏ Ist die Wiederverwendung von Paßwörtern eingeschränkt?

Programm Syscon

❏ Ist das Paßwort in vorzugebenden Zeitabständen zu ändern?

Programm Syscon

❏ Ist die Anzahl der Zugangsberechtigungen nach Paßwortverfall (Grace Login) eingeschränkt?

Programm Syscon

❏ Benötigen Anwender bei ihrer erstmaligen Anmeldung ein neues Paßwort?

Programm Syscon

❏ Werden Anwender nach drei Fehlversuchen automatisch vom System abgemeldet?

Programm Syscon

❏ Ist der Überwachungszeitraum für fehlerhafte Anmeldungen (Retantion Account Period) auf mindestens 15 Minuten eingestellt?

Programm Syscon

❏ Werden Anwender für eine ausreichend lange Zeitspanne bei einer fehlerhaften Paßworteingabe von der Netznutzung ausgeschlossen (Lenth of account logout)?

Programm Syscon

❏ Werden Paßwörter - soweit keine technischen Gegebenheiten dagegen sprechen - ausschließlich verschlüsselt verwendet?

Prüfungshandlungen in Netzwerkumgebungen bei Verwendung verschiedener Betriebssysteme

B. Prüfungshandlung bei Verwendung von NetWare/Novell 3.x

2. Prüfung einer sicheren Administration- und Nutzerverwaltung

❏ Wird für alle User eine UserID und ein Paßwort verlang und wird die Guest-ID nicht für den normalen Netzwerkzugriff verwendet?

❏ Ist die Guest-ID aus der Gruppe Everyone entfernt?

❏ Sind nicht personenbezogene User-ID's gesperrt, werden sie ausschließlich mit Paßwort verwendet oder sind sie ausschließlich auf einen Server beschränkt?

❏ Befinden sich inaktive User im System?

Aufruf des Security Kommandos

❏ Werden Rechte zu Verzeichnissen, die einen umfangreichen Zugriff auf das System ermöglichen, wie z.B. Supervisor oder Operator äußerst restrektiv gehandhabt?

❏ Werden Verzeichnisse mit systemnahen Dateien, wie

- SYS:System
- SYS:Login
- SYS:Public
- SYS:Mail

restriktiv auf Anwender mit Administrator- und Operatorfunktionen beschärnkt?

❏ Ist die auf dem Server installierte Software durch den Befehl SECURE CONSOLE vor unberechtigten Änderungen mittels Utilities geschützt?

❏ Wird das Leserecht (Read) auf Dateien ausschließlich auf hierzu autorisierte Nutzer begrenzt?

❏ Gibt es ein nachvollziehbares transparentes Verfahren für die Zuordnung von Laufwerken zu Usern (Mapping), für das Einrichten von Gruppen, die Zuordnung von Rechten und Personen zu Gruppen (Containern)?

❏ Verfügt das Netzwerk über eine gut organisatorische Struktur mit differenziert zugeordneten Rechten und wird die Gruppe Everyone nicht exzessiv genutzt?

Prüfungshandlungen in Netzwerkumgebungen bei Verwendung verschiedener Betriebssysteme

B. Prüfungshandlung bei Verwendung von NetWare/Novell 3.x

3. Überwachung und Protokollierung

❏ Ist sichergestellt, daß der laufende Systembetrieb ausreichend protokolliert wird?

Programm AuditCon

❏ Werden alle notwendigen systemrelevante Aktvitäten des Supervisors bzw. äquivalenter Anwender regelmäßig ausgewertet?

LTAudit

❏ Werden aus den vorhandenen Logdateien regelmäßig ungewöhnliche bzw. fehlerhafte Zugriffe auf das System aufgezeichnet und ausgewertet?

Programm AuditCon

4. Systemabschottung

❏ Ist die Verschlüsselung des Datenverkehrs (NCP Packet Sign-2) sichergestellt?

❏ Gibt es für jeden Anwender ein Login-Script?

Programm BindView

❏ Wird die Remote-Administration ausreichend abgesichert?

Einstellung zum Remote-Paßwort in der AUTOEXEC.NCF

❏ Ist sichergestellt, daß innerhalb des Netz benötigte Software sicher geladen ist?

Kein BRAKE ON in System-, Profile- und Login-Scripts

❏ Werden Paßwörter verschlüsselt gespeichert und ist der Zugriff auf die Paßwortdateien ausreichend vor unberechtigtem Zugriff geschützt?

❏ Beschränkt sich die Verwendung von RConsole (Remote) sowie von AConsole ausschließlich auf den autorisierten Administrator?

Auswertung des Server Error-Log nach den
Begriffen RConsole und AConsole

❏ Ist die Nachinstallaiton von NLM's (Netware Loadable Moduls) auf dem Server oder von Diskette unmöglich?

Befehl Secure Console

❏ Werden unberechtigte Zugriffsversuche von dem System automatisch aufgezeichnet (Detect Intruder=Yes)?

Prüfungshandlungen in Netzwerkumgebungen bei Verwendung verschiedener Betriebssysteme

C. Prüfung in einer NetWare/Intranet 4.x-Umgebung

1. Schutzeinstellungen zur Paßwortverwendung

❏ Wird für den Netzzugang ein Paßwort benötigt?

Programm NETADMIN

❏ Sind User-ID's vorhanden, die kein Paßwort benötigen?

Programm NETADMIN

❏ Wird regelmäßig auf fehlende Paßwörter geprüft?

Programm SECURITY (System Verzeichnis)

❏ Haben alle Paßwörter eine gewünschte Mindestlänge?

Programm NETADMIN

❏ Ist die Wiederverwendung von Paßwörtern eingeschränkt?

Programm NETADMIN

❏ Ist das Paßwort in vorzugebenden Zeitabständen zu ändern?

Programm NETADMIN

❏ Ist die Anzahl der Zugangsberechtigungen nach Paßwortverfall (Grace Login) eingeschränkt?

Programm NETADMIN

❏ Benötigen Anwender bei ihrer erstmaligen Anmeldung ein neues Paßwort?

Programm NETADMIN

❏ Werden Anwender nach drei Fehlversuchen automatisch vom System abgemeldet?

Programm NETADMIN

❏ Ist der Überwachungszeitraum für fehlerhafte Anmeldungen (Retantion Account Period) auf mindestens 15 Minuten eingestellt?

Programm NETADMIN

❏ Werden Anwender für eine ausreichend lange Zeitspanne bei einer fehlerhaften Paßworteingabe von der Netznutzung ausgeschlossen (Length of account logout)?

Programm NETADMIN

❏ Verfügt der Administrator ADMIN über ein Paßwort (Nach Installation standardmäßig nicht!)?

Prüfungshandlungen in Netzwerkumgebungen bei Verwendung verschiedener Betriebssysteme

C. Prüfung in einer NetWare/Intranet 4.x-Umgebung

1. Schutzeinstellungen zur Paßwortverwendung

❏ Wurden die Administratorrechte auf einen neuen USER übertragen?

❏ Ist der GUEST-ACCOUNT mit restriktiven Rechten (Print only) angelegt?

2. Prüfung einer sicheren Administration- und Nutzerverwaltung

❏ Wird für alle User eine UserID und ein Paßwort verlang und wird die Guest-ID nicht für den normalen Netzwerkzugriff verwendet?

❏ Ist die Guest-ID aus der Gruppe Everyone entfernt?

❏ Sind nicht personenbezogene User-ID's gesperrt, werden sie ausschließlich mit Paßwort verwendet oder sind sie ausschließlich auf einen Server beschränkt?

❏ Befinden sich inaktive User im System?

Aufruf des Security Kommandos aus dem System-Verzeichnis

❏ Werden Rechte zu Verzeichnissen, die einen umfangreichen Zugriff auf das System ermöglichen, wie z.B. Supervisor oder Operator äußerst restriktiv gehandhabt?

❏ Werden Datum und Zeit der letzten Anmeldung bei einem Login angezeigt?

Im Login-Script "DISPLAY LASTLOGINTIME" eintragen

❏ Werden "konkurrierende" USER SESSIONS limitert?

NETADMIN / Concurrent Connections

❏ Werden Verzeichnisse mit systemnahen Dateien, wie

- SYS:System
- SYS:Login
- SYS:Public
- SYS:Mail

restriktiv auf Anwender mit Administrator- und Operatorfunktionen beschärnkt?

❏ Ist die auf dem Server installierte Software durch den Befehl SECURE CONSOLE vor unberechtigten Änderungen mittels Utilities geschützt?

❏ Wird das Leserecht (Read) auf Dateien ausschließlich auf hierzu autorisierte Nutzer begrenzt?

❏ Gibt es ein nachvollziehbares transparentes Verfahren für die Zuordnung von Laufwerken zu Usern (Mapping), für das Einrichten von Gruppen, die Zuordnung von Rechten und Personen zu Gruppen (Containern)?

❑ Verfügt das Netzwerk über eine gut organisatorische Struktur mit differenziert zugeordneten Rechten und wird die Gruppe Everyone nicht exzessiv genutzt?

Prüfungshandlungen in Netzwerkumgebungen bei Verwendung verschiedener Betriebssysteme

C. Prüfung in einer NetWare/Intranet 4.x-Umgebung

3. Überwachung und Protokollierung

❏ Ist sichergestellt, daß der laufende Systembetrieb ausreichend protokolliert wird?

Programm AUDITCON

❏ Werden alle notwendigen systemrelevante Aktvitäten des Supervisors bzw. äquivalenter Anwender regelmäßig ausgewertet?

Programm AUDITCON

❏ Werden aus den vorhandenen Logdateien regelmäßig ungewöhnliche bzw. fehlerhafte Zugriffe auf das System aufgezeichnet und ausgewertet?

Programm AUDITCON, AUDITOR, SECURITY

4. Systemabschottung

❏ Ist die Verschlüsselung des Datenverkehrs?

❏ Gibt es für jeden Anwender ein Login-Script?

Programm AUDITCON

❏ Wird die Remote-Administration ausreichend abgesichert?

Einstellung zum Remote-Paßwort in der AUTOEXEC.NCF

❏ Ist sichergestellt, daß innerhalb des Netz benötigte Software sicher geladen ist?

Kein BRAKE ON in System-, Profile- und Login-Scripts

❏ Werden Paßwörter verschlüsselt gespeichert und ist der Zugriff auf die Paßwortdateien ausreichend vor unberechtigtem Zugriff geschützt?

❏ Beschränkt sich die Verwendung von R-Console (Remote) sowie von A-Console ausschließlich auf den autorisierten Administrator?

Auswertung des Server Error-Log nach den
Begriffen R-Console und A-Console

❏ Ist die Nachinstallaiton von NLM's (Netware Loadable Moduls) auf dem Server oder von Diskette unmöglich?

Befehl Secure Console

❏ Werden unberechtigte Zugriffsversuche von dem System automatisch aufgezeichnet (Detect Intruder=Yes)?

Stichwortverzeichnis

Literaturverzeichnis

IDW	Institut der Wirtschaftsprüfer, Fachausschuß für moderne Abrechnungssysteme (FAMA); Grundsätze ordnungsmäßiger Buchführung bei computergestützten Verfahren und deren Prüfung
IIR	Deutsches Institut für interne Revision e.V., Arbeitskreis "Revision der Datenverarbeitung": DV REVISION, Ergänzbarer Leitfaden zur Durchführung von Prüfungen der Informationsverarbeitung
Odenthal, Roger	Die Prüfung von Netzwerken mit Hilfe einer Revisionssoftware, in ECU-Management, Ausgabe 1, Januar 1994
	EDV-Revision in einer PC-Netzwerkumgebung, in Zeitschrift "Datensicherheits-Report", Ausgabe 7/1996
	EDV-Revision - Unterstützende Verfahren und Instrumente in Zeitschrift "KES", Zeitschrift für Kommunikations- und EDV-Sicherheit, Ausgabe 6, 12/1997
Schuppenhauer, Rainer	Grundsätze für eine ordnungsmäßige Datenverarbeitung (GoDV), IDW-Verlag GmbH, Düsseldorf, 1992
Verschiedene Autoren	LAN, Praxis, WEKA Fachverlag für EDV, Augsburg, 1994
Wißner, Bernd (Hrsg.)	Sichere EDV, Loseblatt-Sammlung, Interest-Verlag, Augsburg, 1994