

Datenschutz bei Windows NT

**Der Hamburgische
Datenschutz-
beauftragte**

**Der Landesbeauftragte
für den Datenschutz der
Freien Hansestadt Bremen**

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Baumwall 7 · 20459 Hamburg · Tel.: (040)428412047 · Telefax: (040)428412372
und dem Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen,
Arndtstraße 1 · 27570 Bremerhaven · Tel.: (0471) 924610 · Telefax: (0471) 9246131
Autoren: Dr. Uwe Schläger, Ulrich Kühn
1. Auflage 2000: 4.000 Exemplare

Druck: Lütcke & Wulff, 20097 Hamburg

Inhaltsverzeichnis

1	Sicherheitsrisiken	4
2	Anforderungen an Betriebssysteme	5
2.1	Grundsutzanforderungen	5
2.2	Zusatzanforderungen	6
3	NT-Architektur	7
4	C2-Sicherheit.....	8
5	Boot-Schutz durch BIOS-Maßnahmen	8
6	Rahmenbedingungen einer sicheren NT-Installation.....	10
6.1	NTFS-Dateisystem.....	10
6.2	Domänenstruktur	10
6.3	Lokale und globale Benutzergruppen	12
6.4	Eingeschränkter Zugriff auf Systemressourcen	12
6.5	Lokale versus zentrale Datenspeicherung	13
7	Administration eines NT-Systems.....	14
7.1	Verwaltung der Zugriffsrechte	14
7.2	Security Account Manager	16
	Abbildung 3: Passwort-Richtlinien im Benutzer-Manager.....	17
7.3	Registry	18
7.4	Protokollierung.....	18
7.5	Rechte des Systemverwalters.....	20
8	NT-Systeme als Bestandteil heterogener Netze.....	21
8.1	Remote Access Service (RAS)	21
8.2	Internetanschluss.....	23
8.3	Systems Management Server (SMS)	26
9	Sicherheitsrelevante Neuerungen von Windows 2000.....	27
9.1	Windows 2000 und Windows NT.....	27
9.2	Encrypting File System (EFS).....	28
9.3	Zugriffsrechte.....	28
9.4	Kerberos	29
9.5	IPSEC.....	29
9.6	Wann ist der Wechsel auf Windows 2000 empfehlenswert?.....	30
	Checkliste zur Prüfung von Windows NT	30
	Bootschutz-Maßnahmen	30
	NT-Installation	30
	NT-Administration.....	31
	Remote Access Service (RAS).....	32
	Internetzugang	32

System Management Service (SMS)..... 32
Quellenhinweise zu Windows NT 33

1 Einleitung

Windows NT hat sich als multitaskingfähiges 32-Bit-Betriebssystem mit einer professionell ausgelegten Systemarchitektur als Standard-Betriebssystem sowohl für Server als auch für Clients etabliert. Zwar vergeht kaum eine Woche, in der von der weltweiten Hackergemeinde keine neuen Sicherheitslücken aufgedeckt und publiziert werden. Dennoch ist Windows NT – entsprechend konfiguriert – aufgrund seiner integrierten Schutzmechanismen dazu geeignet, sowohl unvernetzte als auch vernetzte Arbeitsplatzrechner mit einem relativ hohen Maß an Sicherheit auch ohne zusätzliche Sicherheitssoftware zu betreiben.

Die vorliegende Broschüre versucht in diesem Sinne, das Thema Sicherheit von Windows NT für Administratoren und IuK-Verantwortliche, aber auch für Anwender in verständlicher Weise aufzubereiten. Die Broschüre richtet sich zudem an behördliche und betriebliche Datenschutzbeauftragte sowie an Personal- und Betriebsräte, die sich mit Windows NT aus Sicht des Arbeitnehmerschutzbeschäftigen.

In den ersten beiden Kapiteln werden Sicherheitsrisiken und Anforderungen an Betriebssysteme allgemein formuliert. Anschließend wird in Kapitel 3 und 4 auf die System- und Sicherheitsarchitektur sowie die C2-Klassifikation von Windows NT genauer eingegangen. Welche Aspekte bei der Installation und Administration eines sicheren NT-Systems zu beachten sind, erfährt der Leser in Kapitel 5 und 6, den Hauptkapiteln dieser Broschüre. Auf sicherheitsrelevante Neuerungen von Windows 2000 sowie auf Aspekte, die bei der Einbindung von NT-Systemen in heterogene Netze zu beachten sind, wird in den Schlusskapiteln eingegangen.

2 Sicherheitsrisiken

Mechanismen zum Schutz personenbezogener Daten können sowohl von internen, zugriffsberechtigten Benutzern als auch von externen Personen umgangen werden. Während Externe bereits bei weniger sensiblen Daten ein ernst zu nehmendes Risiko darstellen, ist dies bei Internen nur bei sensiblen personenbezogenen Daten der Fall. Allerdings besitzen interne Mitarbeiter meistens mehr Zugriffsrechte bzw. Kenntnisse über die technischen Details und haben deswegen größere Möglichkeiten, bestehende Schwachstellen auszunutzen. Die Trennlinie zwischen intern und extern verläuft jedoch in größeren Organisationseinheiten innerhalb der Organisation. Mitarbeiter, die bestimmte personenbezogene Daten nicht zur Ausführung ihrer Tätigkeit benötigen, sind in diesem Sinne ebenso Externe wie nicht der Organisation zugehörige Dritte.

Auf der Ebene des Betriebssystems kann zwischen folgenden Risiken differenziert werden:

1. Arbeiten unter falscher Identität:

Gegenüber dem Betriebssystem kann unter einer falschen Identität agiert werden, um sämtliche Privilegien des rechtmäßigen Benutzers zu übernehmen und auf dessen Daten zuzugreifen. Entweder wird bereits bei der Benutzerauthentifizierung das Passwort einer anderen Person verwendet, das vorab möglicherweise aus einer ungesicherten Passwortdatei ausgelesen wurde. Eine andere Möglichkeit besteht darin, erst nach der regulären Anmeldung dauerhaft die interne Repräsentation eines anderen Benutzers anzunehmen.

2. Erweiterung von Rechten:

Schwachstellen im verwendeten Betriebssystem können ausgenutzt werden, um zusätzliche Rechte unter der eigenen Identität zu gewinnen.

3. Umgehen des Betriebs- und Sicherheitssystems:

Sicherheitsmechanismen können vollständig umgangen werden, falls es gelingt, ein anderes oder ein anders konfiguriertes Betriebssystem zu laden, beispielsweise durch die Möglichkeiten, unauthorisiert auf den Systemstart und das Laden des Betriebssystems einzuwirken.

4. Abhören von Geräten:

Die kompromittierende Strahlung von Bildschirmen und anderen Geräte kann dazu genutzt werden, die dort verarbeiteten Daten oder Zugangsinformationen aus gewisser Entfernung abzuhören. Der für ein Abhören der Abstrahlung erforderliche Aufwand ist allerdings beträchtlich.

5. Verwischen von Spuren:

Systemseitig erstellte Protokolldateien können verändert werden, um die Spuren eines missbräuchlichen Zugriffs auf personenbezogene Daten zu beseitigen.

6. Missbräuchliche Nutzung von Netzwerkverbindungen:

Vernetzte Rechner unterliegen prinzipiell dem Risiko, dass über bestehende Netzwerkverbindungen unberechtigt von außen zugegriffen oder auf das Systemverhalten Einfluss genommen werden kann.

3 Anforderungen an Betriebssysteme

Anforderungen werden in dieser Broschüre – soweit dies möglich ist – auf der Basis eines zweistufigen Grundschutzkonzepts formuliert. Die Grundschutzmaßnahmen sollen einen Mindest-Sicherheitsstandard garantieren, der es ermöglicht, personenbezogene Daten mit einem geringen Schutzbedarf unter Windows NT zu verarbeiten. Falls sensible personenbezogene Daten gespeichert werden, beispielsweise medizinische Daten, Sozialdaten oder Personaldaten, ist es notwendig, über die Grundschutzmaßnahmen hinaus zusätzliche Maßnahmen zu treffen.

Die Grundschutzmaßnahmen richten sich weitgehend gegen den Missbrauch personenbezogener Daten durch Externe (externer Missbrauch). Als Externe gelten aus Sicht einer Organisation nicht nur Außenstehende, sondern auch diejenigen Benutzer, die für eine Anwendung oder die Nutzung eines Datenbestandes nicht autorisiert sind. Grundschutzmaßnahmen sind daher nicht gegen den zugriffsberechtigten Benutzer gerichtet. Die zum Schutz sensibler Daten erforderlichen Zusatzmaßnahmen sind darüber hinaus in der Lage, personenbezogene Daten vor unberechtigter Weitergabe oder missbräuchlicher Nutzung durch Interne zu schützen, d.h. auch durch die jeweils berechtigten Benutzer (interner Missbrauch).

3.1 Grundschutzanforderungen

Authentisierung der Benutzer

Zunächst ist es notwendig, sämtliche Benutzer eindeutig zu identifizieren. Nur wenn die Identität eines Benutzers zweifelsfrei feststeht, können an den Benutzer gekoppelte Berechtigungsprofile greifen. Die zweifelsfreie Authentisierung setzt geeignete Mechanismen wie Passworteingabe, den Besitz einer Chipkarte oder biometrische Verfahren voraus.

Um zu verhindern, dass Passwörter erraten oder ausspioniert werden, sollten die verwendeten Passwörter regelmäßig und automatisiert auf ihre Mindestlänge, ihre begrenzte zeitliche Gültigkeit, ihre Ungleichheit mit vorherigen Passwörtern und ihre Nicht-Trivialität überprüft werden. Es sollten ausschließlich individuelle Passwörter und keine Gruppenpasswörter verwendet werden; auch sollten die Passwörter nicht dem Systemverwalter bekannt sein. Passwörter die beispielsweise im Vertretungsfall Dritten bekannt geworden sind, sollten unverzüglich geändert werden.

In Client-Server-Umgebungen kann sich der Benutzer entweder lokal oder gegenüber dem Netz authentisieren. Dabei sollte das Ergebnis der lokalen Authentisierung – ihre Wirksamkeit vorausgesetzt – fälschungssicher an andere Netzrechner weitergegeben werden können. Hierdurch wird verhindert, dass der Benutzer auf jeder Systemebene ein separates Passwort verwenden muss. Mehrere Passwörter erhöhen weder die Gesamtsicherheit des Systems noch sind sie benutzerfreundlich – die Sicherheit der Systeme wird vielmehr reduziert. Welcher Benutzer kann sich schon drei verschiedene, regelmäßig zu ändernde Passwörter merken? Werden jedoch auf allen Ebenen identische Passwörter benutzt, ist das Gesamtsystem nur so sicher wie seine schwächste Authentisierungskomponente.

Differenzierte Vergabe der Zugriffsrechte

Falls beim Mehrbenutzer-Betrieb mehrere Personen mit unterschiedlichen Arbeitsaufgaben auf einen Rechner zugreifen, sollten die Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Verzeichnisse und Dateien anderer Benutzer sollten weder gelesen noch verändert werden können. Zugriffsrechte sollten daher auf Verzeichnis- und Dateiebene sowohl für einzelne Benutzer als auch für Benutzergruppen abgestuft vergeben werden können, möglichst noch differenziert nach Lese-, Schreib- und Ausführungsrechten. Im Einbenutzerbetrieb kann dagegen auf die differenzierte Vergabe von Zugriffsrechten verzichtet werden. Hier reicht es aus, den unberechtigten Zugriff auf das System insgesamt zu verhindern.

Zugriffsrechte sollten im Client-Server-Betrieb arbeitsplatzbezogen an ein bestimmtes Endgerät oder eine Gruppe von Endgeräten gebunden werden können. Zudem sollte es möglich sein, die Zugriffsberechtigung zeitlich einzuschränken und die Zahl der Anmeldungen pro Benutzerkennung zu begrenzen. Dem Systemverwalter sollte trotz seines privilegierten Status der Zugriff auf personenbezogene Daten verwehrt werden können.

3.2 Zusatzanforderungen

Restriktive Nutzung der Systemressourcen

Benutzer sollten nur einen beschränkten Zugriff auf Betriebssystemressourcen erhalten. Diskettenlaufwerke, CD-ROM-Laufwerke, serielle und parallele Schnittstellen sollten nur insoweit benutzt werden können, wie dies zur Aufgabenerledigung erforderlich ist.

Systemressourcen sollten auch den Systemverwaltern nur soweit zur Verfügung gestellt werden, wie dies für die jeweilige Aufgabe notwendig ist. Tätigkeiten wie beispielsweise das Einrichten von Benutzern, das Ändern von Passwörtern bzw. das Erstellen von Tagessicherungen benötigen keine privilegierten, allumfassenden Zugriffsrechte. Uneingeschränkter Betriebssystemzugriff sowie der Zugriff auf weitere Betriebsmittel wie Compiler und Debugger ist dagegen nur für die wenigsten Systemverwaltertätigkeiten notwendig.

Datenverschlüsselung

Um vor Diebstahl geschützt zu sein, sollten sensible personenbezogene Daten auf wechselbaren Datenträgern verschlüsselt gespeichert werden. Auf der Festplatte hinterlegte Daten sollten dann verschlüsselt werden, wenn das Risiko besteht, dass entweder die Festplatte oder der gesamte PC entwendet werden (z.B. bei Laptops).

Sofern sensible personenbezogene Daten über öffentliche Netze übertragen werden, ist es in jedem Fall notwendig, die Daten verschlüsselt zu übertragen. Die Verschlüsselung der Daten kann entweder auf Übertragungsebene, auf Netzwerkebene oder auf Anwendungsebene erfolgen. Bei der Verbindungsverschlüsselung werden die Daten nur zwischen bestimmten Netzwerkrechnern ungeachtet des Absenders oder Empfängers chiffrieren. Verfahren zur Ende-zu-Ende-Verschlüsselung chiffrieren die Daten dagegen auf der gesamten Strecke zwischen Absender und Empfänger und benutzen dabei individuelle Schlüssel.

Protokollierung

Es sollten sowohl sicherheitsrelevante Benutzer- als auch Systemaktivitäten protokolliert werden. Sicherheitsrelevante Benutzeraktivitäten sind vor allem fehlgeschlagene Anmeldeversuche, Zugriffe auf Dateien mit sensiblen personenbezogenen Daten, der Aufruf bestimmter Programme, die zur Auswertung personenbezogener Daten benötigt werden, versuchte Rechteüberschreitungen, das Kopieren auf externe Datenträger sowie Datenübermittlungen. Sicherheitsrelevante Systemaktivitäten, die in der Regel vom Systemverwalter mit privilegierten Zugriffsrechten ausgeführt werden, sind das Einrichten von Benutzerkennungen bzw. -gruppen, das Ändern von Passwörtern, die Freigabe von Programmversionen sowie das Modifizieren von datensicherungstechnisch relevanten Systemparametern.

Es sollte darauf geachtet werden, dass die Protokolldaten nicht unbemerkt verändert oder gelöscht werden können, auch nicht durch den Systemverwalter. Da die Protokolle u.a. zur Transparenz der Systemverwaltung dienen, sollten die Protokolldaten von Personen ausgewertet werden, die nicht direkt für die Systemverwaltung verantwortlich sind. Die Auswertung der Protokolle sollte möglichst nach dem Vier-Augen-Prinzip in Anwesenheit zweier Personen durchgeführt werden, die sich beide gegenüber dem System authentisieren müssen. Um Bedenken von Arbeitnehmervertretern auszuräumen, dass Protokolle nicht nur zur Systemrevision, sondern auch zu Leistungs- und Verhaltenskontrollen zweckentfremdet genutzt werden, kann es sinnvoll sein, an der Protokollauswertung entweder Vertreter des Personal- oder Betriebsrats oder den betrieblichen Datenschutzbeauftragten zu beteiligen.

4 NT-Architektur

Windows NT basiert auf einer Architektur, bei der der Benutzerbereich (User-Mode) strikt von dem geschützten Systembereich (Kernel-Mode) getrennt ist. Der Systembereich (sog. Executive) ist von den im Benutzermodus ablaufenden Subsystemen für 32-Bit- und 16-Bit-Applikationen vollständig unabhängig. Jedes Subsystem verfügt über einen eigenen Speicherbereich und kommuniziert mit anderen Subsystemen sowie mit dem Kernel ausschließlich über definierte Schnittstellen. Diese Abschottung des Systemkerns wirkt sich positiv auf die Stabilität und Zuverlässigkeit des Systems aus. Sie verhindert insbesondere die Beeinträchtigung des Gesamtsystems durch einzelne Applikationen.

Innerhalb des User-Mode übernimmt das Sicherheitssubsystem Local Security Authority (LSA) in Verbindung mit dem Security Account Manager (SAM) diverse Sicherheitsaufgaben, wie die Verwaltung der lokalen Sicherheitspolitik, die Bereitstellung von Diensten zur Benutzeridentifikation und -authentisierung, Chiffrierung der Passwörter und die Erzeugung und Pflege der Protokolldateien.

Dieses Sicherheitssubsystem wird durch den sog. Security Reference Monitor (SRM) innerhalb der Executive ergänzt. Dieser beinhaltet und kontrolliert einheitlich und netzwerkweit sicherheitsrelevante Funktionen, wie beispielsweise die Überprüfung von Benutzerzugriffen auf die unterschiedlichen NT-Objekte (Dateien, Verzeichnisse, Kataloge, Prozesse, Speicherbereiche, Geräte, etc.).

5 C2-Sicherheit

Windows NT, so ist häufig zu hören, sei ein sicheres Betriebssystem, da es von nordamerikanischen Sicherheitsbehörden nach der Sicherheitsstufe C2 zertifiziert sei. Folglich sei man als Anwender von Windows NT immer auf der sicheren Seite. Dies ist jedoch nur bedingt richtig.

Zum einen wurde bislang lediglich die Workstation-Version zertifiziert. Zwar sind in amerikanischen Guidelines zur NT-Sicherheit zahlreiche Sicherheitsmechanismen aufgelistet, die es dem Systemverwalter ermöglichen, auch für die Server-Version einen C2-ähnlichen Sicherheitsstandard zu erreichen (z.B. Secure Windows NT Installation und Configuration Guide der US Navy, Windows NT Security Guidelines der NSA). Microsoft stellt im Service Pack 3 hierzu einen C2-Konfiguration Manager zur Verfügung, der den Systemverwalter in dieser Hinsicht unterstützt. Dennoch fehlt für die Serverversion von Windows NT weiterhin ein entsprechendes Zertifikat.

Zum anderen orientieren sich Kriterien wie beispielsweise C2 zum Teil an Zielen militärischer Sicherheit, die nicht immer deckungsgleich mit den Anforderungen sind, die Systemverwalter und Datenschutzbeauftragte an die Sicherheit der Systeme stellen. Der Begriff der C2-Sicherheit wurde nicht zuletzt vom nordamerikanischen Verteidigungsministerium erstmals zu Beginn der achtziger Jahre in einem sogenannten Orange Book verwendet, hat allerdings seitdem auch die Diskussion um Sicherheitskriterien europa- und weltweit geprägt: Identifikation und Authentisierung, Rechteverwaltung, Rechteprüfung, Beweis-sicherung, Wiederaufbereitung, Fehlerüberbrückung, Gewährleistung der Funktionalität sowie Übertragungssicherung sind acht Grundfunktionen, die ein sicheres System nach den Vorstellungen des Orange Book zur Verfügung stellen sollte.

Zudem sind Kriterien wie C2 teilweise sehr abstrakt formuliert. Der Umfang und die Tiefe der Kriterien erfordern komplexe Systemprüfungen, die sowohl in qualitativer als auch in quantitativer Hinsicht nur von wenigen Firmen durchgeführt werden können. Die Zertifizierungen dauern daher meistens mehrere Monate. Da die Zertifikate auch nur für einzelne Versionen gelten, müssen neuere Versionen nachzertifiziert werden, wenn das Zertifikat auch weiterhin Gültigkeit besitzen soll. Dies ist selbst für große DV-Hersteller mit einem umfangreichen Produktangebot über einen längeren Zeitraum nicht immer leistbar.

Auch die in Kapitel 2 dieser Broschüre formulierten Anforderungen orientieren sich teilweise an den genannten Grundfunktionen des Orange Book. Allerdings sind die Anforderungen nicht nur auf den Missbrauch durch Aussenstehende gerichtet, sondern wirken entgegen der Orange-Book- und Common-Criteria-Sichtweise auch Risiken entgegen, die von den Benutzern oder den Systemverwaltern selbst ausgehen können.

6 Boot-Schutz durch BIOS-Maßnahmen

Nicht alle der in Kap. 2 formulierten Anforderungen können ausschließlich auf Betriebssystemebene umgesetzt werden. Um nach dem Anschalten des Arbeitsplatz-PC zu garantieren, dass die lokalen Sicherheitsmechanismen von Windows NT auch zum Zuge kommen, müssen auf BIOS-Ebene entsprechende Maßnahmen getroffen werden. Sofern es beispielsweise gelingt, den NT-Rechner unter MS-DOS zu starten, können sämtliche lokalen NT-Mechanismen umgangen wer-

den. Es existieren frei verfügbare Programme, die es unter MS-DOS ermöglichen, NTFS-formatierte Datenträger ohne Zugriffsbeschränkung zu lesen und zu manipulieren. Auch kann über das CD-ROM-Laufwerk eine Neuinstallation durchgeführt werden, so dass bestehende Sicherheitseinstellungen außer Kraft gesetzt werden.

Aus diesem Grund sollte auf dem Rechner neben NT kein weiteres Betriebssystem zur Verfügung stehen. Das Booten von Diskette oder CD-ROM sollte durch entsprechende Konfiguration des Basic Input Output System (BIOS) verhindert werden. Um auszuschließen, dass die restriktiv wirkenden BIOS-Einstellungen nicht unbefugt verändert werden, sollte das BIOS nur nach vorheriger Passwordeingabe konfiguriert werden können. Auf die generelle Passwortabfrage beim Systemstart auf BIOS-Ebene kann dagegen verzichtet werden, da die Authentisierung des Benutzers durch Windows NT vorgenommen wird.

Allerdings gibt es Möglichkeiten, die Schutzwirkungen von BIOS-Einstellungen auch ohne Kenntnis des BIOS-Passwort wieder aufzuheben. Zum einen besteht die Möglichkeit, die BIOS-Einträge durch Manipulation der Hardware zu löschen. Die BIOS-Einträge werden in CMOS-RAM-Bauteilen gespeichert, die eine ständige Stromversorgung benötigen. Wird diese Stromversorgung unterbrochen, werden die sicherheitsrelevanten Einträge einschließlich des BIOS-Passwortes gelöscht. Es sollten daher Maßnahmen wie Gehäuseschlösser getroffen werden, die ein Öffnen des Gerätes verhindern, wenn ein unbeobachteter unberechtigter Zugang zu dem PC nicht ausgeschlossen werden kann.

Zum anderen existieren zahlreiche Softwareprogramme, mit denen die BIOS-Konfiguration geändert und das Passwort ausgelesen werden können. Beispielsweise kann mit Hilfe des zur Standard-Installation von Windows NT gehörenden Programms Q-BASIC das gesamte CMOS gelöscht werden, so dass sämtliche Einstellungen im BIOS verloren gehen. Das gleiche lässt sich mit dem Microsoft-Programm DEBUG.EXE erzielen, das ebenfalls zur Standardinstallation eines Windows-Betriebssystems gehört. Die Eingabe einer bestimmten Sequenz bewirkt, dass das BIOS-Passwort gelöscht wird und somit die BIOS-Parameter ohne Eingabe des BIOS-Passwortes bearbeitet werden können.

Darüber hinaus sind einige Crack-Programme im Internet verfügbar, die versuchen BIOS-Passwörter auszuprobieren. Da das Passwort bei einigen BIOS-Systemen (z.B. AWARD-BIOS) durch eine Hash-Funktion lediglich auf 2 Byte reduziert und abgespeichert wird, sind solche Programme relativ schnell erfolgreich. Dabei kann sich das erratene Passwort deutlich vom Originalpasswort unterscheiden. Die Crack-Programme generieren solange Zeichenfolgen, bis deren Hash-Wert dem gespeicherten Wert identisch ist. Für das Erraten von Passwörtern mit Hilfe derartiger Crack-Programme ist die Länge und die Qualität des Originalpasswortes unerheblich. Auch für 8-stellige Originalpasswörter, die aus Buchstaben, Ziffern und Sonderzeichen zusammengesetzt sind, können sehr schnell Zeichenfolgen ermittelt werden, die auf den gleichen 2 Byte-Hashwert abgebildet werden.

Der Einsatz von Software zur Manipulation von BIOS-Einträgen setzt zwar die Inbetriebnahme des Gerätes voraus und ist insofern unproblematisch, wenn durch BIOS-Maßnahmen Aussenstehende vom Rechner ferngehalten werden sollen. In den Fällen, in denen je-

doch das Laden eines anderen Betriebs-systems durch den berechtigten Benutzer selbst verhindert werden soll, stellen derartige Programme gleichwohl ein Problem dar.

Allerdings können Manipulationen des BIOS zumindest nachträglich erkannt werden, da das BIOS-Passwort entweder verändert oder gelöscht wurde. Programme wie Q-BASIC und DEBUG, die im allgemeinen vom Benutzer nicht benötigt werden, sollten gleichwohl nicht auf dem Arbeitsplatz-PC verfügbar sein.

7 Rahmenbedingungen einer sicheren NT-Installation

In diesem Kapitel wird auf Sicherheitsmechanismen eingegangen, die bereits sehr frühzeitig bei der Erstinstallation und Anfangskonfiguration von NT-Systemen beachtet werden sollten und die zu einem späteren Zeitpunkt nur umständlich zu korrigieren sind. Insbesondere sollten folgende Fragen beantwortet werden:

- Welches Dateiformat soll benutzt werden?
- Welches Domänenmodell (Ein-Domänen- oder Master-Domänen-Modell) kommt für die Organisation in Frage?
- Welche Programme bzw. Anwendungen sollen lokal oder zentral installiert werden?
- Sollen die personenbezogenen Daten lokal oder ausschließlich zentral abgelegt werden?

7.1 NTFS-Dateisystem

Ein wesentlicher Baustein innerhalb der NT-Sicherheitsarchitektur ist das Dateisystem. Windows NT ermöglicht die Arbeit mit drei verschiedenen Dateisystemen:

- **FAT** ist das von MS-DOS übernommene Dateisystem. Dieser Kompatibilitäts-vorteil stellt sich jedoch insofern als großer Nachteil dar, als FAT-formatierte Datenträger aufgrund fehlender Dateiattribute ohne Zugriffsbeschränkung gelesen und verändert werden können.
- **HPFS** ist das für das Betriebssystem OS/2 ab Version 1.2 entwickelte Dateisystem. Es weist zwar einige Verbesserungen gegenüber dem Dateisystem FAT auf, bietet jedoch keine wesentlichen Sicherheitsvorteile.
- **NTFS** wurde speziell für Windows NT entwickelt. Neben längeren Dateinamen und einem schnelleren Zugriff auf große Dateien unterscheidet sich NTFS von den anderen Formaten vor allem durch die erweiterten Dateiattribute, mit denen die Zugriffsrechte individuell bis auf die Dateiebene gesteuert werden können.

Ein datenschutzkonformer Betrieb kann folglich nur garantiert werden, wenn bei der Einrichtung eines NT-Systems das NTFS-Dateisystem benutzt wird.

7.2 Domänenstruktur

Domänen bilden die grundlegende Einheit beim Betrieb von NT-Netzen. Das Zusammenfassen von NT-Servern zu Domänen ist sowohl für Netzwerkadministratoren als auch für Benutzer vorteilhaft. Für jede Domäne wird eine gemeinsame Datenbank mit Benutzerkonten, Gruppenkonten und Sicher-

heitseinstellungen erstellt. Der Administrator muss innerhalb einer Domäne für jeden Benutzer nur ein Benutzerkonto verwalten, einzelne Server-Konten werden dadurch vermieden.

In einem Netzwerk können mehrere Domänen voneinander unabhängig oder durch Vertrauensbeziehungen mit einander verknüpft installiert werden. Durch Vertrauensbeziehungen lässt sich in einem Netzwerk mit vielen Domänen ein Duplizieren der Benutzerkonten vermeiden und das Risiko uneinheitlicher Kontoinformationen verringern. Gleichzeitig besteht jedoch die Gefahr, dass der Überblick über Berechtigungen sowohl für globale Gruppen als auch für einzelne Benutzer bei vielfältigen Vertrauensbeziehungen verloren geht.

Die Auswahl des Domänenmodells sollte bei der Planung eines NT-Netzes getroffen werden. Dabei sind unterschiedliche Domänen-Modelle denkbar.

1. Ein-Domänen-Modell:

Beim Ein-Domänen-Modell ist nur eine einzelne Domäne vorhanden; es bestehen keine Vertrauensbeziehungen zu anderen Domänen. Sämtliche Benutzer melden sich nur innerhalb dieser Domäne an. Das Ein-Domänen-Modell ist geeignet für kleine bis mittelgroße Netze. Es ist dadurch gekennzeichnet, dass alle Benutzerdaten zentral verwaltet werden. In großen Netzen stößt dieses Modell an technische und organisatorische Grenzen.

Wenn zahlreiche Benutzer und Rechner in einer einzigen Domäne verwaltet werden, besteht das Risiko einer Fehladministration aufgrund zunehmender Unübersichtlichkeit.

2. Master-Domänen-Modell:

Beim Modell der Master-Domäne existieren mehrere Domänen, die sämtlich der sogenannten Master-Domäne vertrauen, die aber ihrerseits keiner der übrigen Domänen vertraut. Das Master-Domänen-Modell ermöglicht es, mehrere Domänen unabhängig voneinander einzurichten, sie jedoch zentral zu verwalten. Fachabteilungen haben in der Regel ausschließlichen Zugriff auf ihre eigenen Ressourcen; die Benutzerkonten müssen jedoch nur einmal in der Master-Domäne definiert werden. Um im Falle einer Fehlfunktion des Primary-Domain-Controller (PDC) die Funktionsfähigkeit des Netzes gewährleisten zu können, sollte beim Modell der Master-Domäne zumindest ein Backup-Domain-Controller (BDC) eingerichtet sein.

3. Mehrfach-Master-Domänen:

Bei diesem Modell werden mehrere Master-Domänen eingerichtet, die sich untereinander vertrauen. Alle anderen Domänen vertrauen diesen Master-Domänen, allerdings vertraut in umgekehrter Richtung keine der Master-Domänen den restlichen Teildomänen. Das Mehrfach-Master-Domänenmodell wird häufig von großen Unternehmen gewählt, um die Benutzerverwaltung in einer kleinen Anzahl von Masterdomänen, die als Kontendomänen fungieren, zu konzentrieren. Die eigentlichen NT-Ressourcen werden von Domänen verwaltet, die sich unterhalb dieser Master-Domänen befinden.

4. Vollständiges Vertrauens-Modell:

Alle Domänen vertrauen sich vollständig untereinander. Es existiert keine Master-Domäne, die die Benutzerverwaltung für alle anderen Domänen zentral übernimmt; die Verwaltung der Benutzer verteilt sich auf viele Domänen. Dieses Modell ist allerdings schwierig zu verwalten, sobald viele Domänen eingerichtet werden müssen, so dass das Modell aufgrund der Anzahl von Vertrauensstellun-

gen für Großunternehmen ungeeignet ist. Das vollständige Vertrauens-Modell lässt sich nur dann sicher administrieren, wenn wenige Netzwerk-Domänen existieren.

Neben der domänenorientierten Vernetzung auf Client-Server-Basis können unter Windows NT auch serverlose Peer-to-Peer-Netzwerke gebildet werden. Innerhalb einer solchen Arbeitsgruppe verwaltet jeder Computer seine eigenen Benutzer- und Gruppenkonten bzw. seine eigenen Sicherheitsrichtlinien und Datenbanken für Sicherheitskonten; diese sind nicht für andere Computer freigegeben. Gegenüber anderen Rechnern der Arbeitsgruppe muss sich der Benutzer daher immer mit seiner NT-Kennung und seinem Passwort anmelden. Es findet kein Austausch der Authentisierungsinformationen zwischen den jeweiligen Rechnern statt. Arbeitsgruppen sind deshalb nur für kleine Gruppen von Computern mit relativ wenigen Benutzerkonten ohne zentrale Netzwerkverwaltung zu empfehlen.

NT-Netze, in denen sensible personenbezogene Daten verarbeitet werden, sollten möglichst nur als Domäne betrieben werden. NT-Domänen, in denen sensible personenbezogene Daten verarbeitet werden, sollten möglichst nicht Domänen anderer Stellen vertrauen.

7.3 Lokale und globale Benutzergruppen

Jede Person, die auf Ressourcen einer Domäne zugreifen möchte, benötigt ein Benutzerkonto in der Domäne des Netzwerkes. Zur Vereinfachung und übersichtlicheren Gestaltung der Netzwerkverwaltung sollten vom Administrator Benutzergruppen für solche Benutzer eingerichtet werden, die Anwendungsprogramme gemeinsam benutzen, ähnliche Aufgaben ausführen oder ähnliche Informationen benötigen. Die Rechte für die einzelnen Benutzer, die Mitglied in der Gruppe sind, müssen dann nur einmal pro Gruppe vergeben und gepflegt werden. Es empfiehlt sich, den einzelnen Gruppen separate Verzeichnisbereiche zuzuweisen. Ein Benutzer kann dabei auch Mitglied mehrerer Gruppen sein.

Bei Benutzergruppen unterscheidet man zwischen lokalen und globalen Gruppen. Eine lokale Gruppe steht nur auf dem jeweiligen PC zur Verfügung, auf dem sie eingerichtet wurde, während eine globale Gruppe in der eigenen und allen vertrauenden Domänen verfügbar ist. Eine globale Gruppe enthält lediglich einzelne Benutzerkonten, keine weiteren Gruppen aus der jeweiligen Domäne, in der sie eingerichtet wurde. Eine lokale Gruppe umfasst dagegen eine Anzahl von Benutzern und globalen Gruppen aus einer oder mehreren Domänen, die unter einem Gruppennamen zusammengefasst werden. Der Gruppe können nur Rechte und Privilegien innerhalb der eigenen Domäne zugewiesen werden.

7.4 Eingeschränkter Zugriff auf Systemressourcen

Sofern sensible personenbezogene Daten verarbeitet werden, sollte der Benutzer möglichst nur diejenigen Anwendungen aufrufen bzw. Systemressourcen nutzen können, die zur eigentlichen Aufgabe benötigt werden. Ansonsten besteht die Gefahr, dass Software per Diskette oder CD-ROM oder per elektronischer Post nachgeladen und aufgerufen wird, mit deren Hilfe Sicherheitsmechanismen direkt oder indirekt unterlaufen werden können.

Die Forderung nach Sperrung nicht benötigter Arbeitsmittel sollte zwar nicht dazu führen, dass der PC nur noch sehr restriktiv genutzt werden kann und kaum mehr als flexibles Arbeitsmittel zur Verfügung steht. Umgekehrt darf das durchaus berechtignte Interesse eines jeden Beschäftigten, un-abhängig vom konkreten

Anwendungsbedarf elektronische Post und Internetzugang nutzen zu können, jedoch nicht zur Folge haben, dass ein derartiger Infrastrukturansatz mit allen damit verbundenen Sicherheitsrisiken sorglos an jedem Arbeitsplatz umgesetzt wird.

Die Frage, welche Arbeitsmittel zur Verfügung gestellt werden, sollte daher für jede Anwendung problembewusst entschieden werden. Dabei muss auch dem PC-Benutzer mehr Verantwortung hinsichtlich lokaler Sicherheit übertragen werden. Inwieweit dies möglich ist, kann allerdings nicht anwendungsübergreifend durch Standardlösungen vorgegeben werden.

Systemressourcen können auf Hardware- bzw. BIOS-Ebene oder auf NT-Ebene eingeschränkt werden. Disketten- und CD-ROM-Laufwerke lassen sich im Registry-Teilschlüssel *HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon* sperren, indem die Werte *AllocateFloppies* bzw. *AllocateCDRoms* auf den DWORD-Wert 1 gesetzt werden. Das Deaktivieren ist jedoch nur für den gesamten Rechner möglich, nicht differenziert für einzelne Benutzer, so dass der Systemadministrator erst die entsprechenden Registry-Einträge zurücksetzen muss, wenn er über das CD-ROM-Laufwerk Software installieren will.

Ebenfalls im Registry-Teilschlüssel *HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon* sollte die Möglichkeit eingeschränkt werden, NT-Server zu beenden. Sofern der Wert *ShutdownWithoutLogon* auf den Wert 1 gesetzt ist, kann das System nur von hierfür autorisierten Benutzern heruntergefahren werden.

NT-seitig kann der netzweite Zugriff auf Systemressourcen auch durch den Systemrichtlinien-Editor *poledit* definiert und eingeschränkt werden; dies gilt insbesondere für

- den Zugriff auf die Systemsteuerung,
- die Gestaltungsmöglichkeiten der Arbeitsumgebung,
- bestimmte Teile der Netzwerkeinstellungen,
- bestimmte Teile der Desktop-Anpassung,
- den Zugriff auf Programme bzw. Anwendungen.

Die Arbeitsumgebung eines Benutzers sollte bei Anwendungen mit sensiblen personenbezogenen Daten derart einschränkt werden, dass dieser keinen Zugriff auf die Eingabeaufforderung *Ausführen* hat, sondern nur Zugriff auf bestimmte Anwendungen. Die Systemrichtlinie muss im Verzeichnis *WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS* unter dem Namen *NTCONFIG.POL* abgelegt werden.

Diese Richtlinien können auf den Standardbenutzer, einzelne Benutzer oder ganze Benutzergruppen angewandt werden. Ebenso können Richtlinien für den Standardcomputer oder für einzelne, mit einem Namen versehene Computer erzeugt werden. Die Standardcomputer-Einstellungen werden angewandt, wenn sich ein neuer Benutzer auf einem Rechner anmeldet, dem keine individuellen Richtlinien zugewiesen wurden.

7.5 Lokale versus zentrale Datenspeicherung

Personenbezogene Daten sind auf einer räumlich ungesicherten NT-Workstation in der Regel nicht so sicher aufgehoben wie auf einem NT-Server, der in einem verschlossenen Raum untergebracht ist. Lokale Festplatten oder der gesamte Arbeits-

platz-PC können entwendet und die darauf hinterlegten Daten – sofern sie unverschlüsselt gespeichert sind – von Außenstehenden ausgelesen werden. Auch kann aufgrund der begrenzten Sicherheitsmechanismen, die auf BIOS-Ebene zur Verfügung stehen, ein Laden anderer Betriebssysteme und das Umgehen der Zugriffsbeschränkungen vor Ort nicht ausgeschlossen werden (vgl. Kap. 5).

Angesichts dieser Risiken, sollten sensible personenbezogene Daten – sofern ein Client-Server-Netzwerk zur Verfügung steht – nicht lokal auf einem Arbeitsplatz-PC gespeichert werden. Die Daten sollten stattdessen auf einem NT-Server hinterlegt sein, der durch geeignete räumliche Sicherheitsmaßnahmen vor fremdem Zugang geschützt ist. Bei unverbundenen Arbeitsplatz-PC sollte zusätzlich zu Windows NT geeignete Sicherheitssoftware eingesetzt werden, die es u.a. ermöglicht, die sensiblen personenbezogenen Daten lokal zu verschlüsseln.

8 Administration eines NT-Systems

In diesem Kapitel wird genauer darauf eingegangen, welche Aspekte bei der Administration eines NT-Systems zu beachten sind. Insbesondere werden folgende Fragen thematisiert:

- Welche Zugriffsrechte können für einzelne Benutzer vergeben werden?
- Welche Rechte sollen die Administratoren erhalten?
- Welche System- und Benutzeraktivitäten sollen protokolliert werden?
- Wie schütze ich herausgehobene NT-Ressourcen wie die Registry oder SAM-Datei?

8.1 Verwaltung der Zugriffsrechte

Ein Benutzer kann unter Windows NT nur dann arbeiten, wenn für ihn ein Benutzerkonto eingerichtet ist, unter dem er sich anmelden kann. Abhängig von der Wahl des Domänen-Modells wird das Benutzerkonto entweder lokal auf einer NT-Workstation oder auf einem Primary Domain Controller angelegt. In dem Benutzerkonto werden die Zugriffsrechte für NT-Ressourcen definiert (Dateien, Drucker, etc.) sowie ein Passwort eingerichtet.

Für die verschiedenen Windows-NT-Objekte können für jeden Benutzer und jede Benutzergruppe differenzierte Zugriffsrechte vergeben werden: Read (R), Write (W), Execute (X), Delete (D), Change Permission (P), Take Ownership (O). Benutzer können gleichzeitig mehreren Gruppen angehören, so dass sich hierüber abgestufte, jedoch auch sehr komplexe und teilweise schwer durchschaubare Rechteverteilungen aufbauen lassen. Windows NT fasst für Verzeichnisse und Dateien die oben genannten Berechtigungen zu folgenden Standardberechtigungen zusammen, die die häufigsten Zugriffsarten abdecken:

Zugriffsart	Beschreibung
Kein Zugriff (keine Rechte)	Verhindert jeden Zugriff auf den Inhalt des Verzeichnisses, seine Unterverzeichnisse und Dateien.

Anzeigen (R)	Der Inhalt des Verzeichnisses (Unterverzeichnisse und Dateien) wird angezeigt, ein Zugriff auf die Daten ist jedoch nicht möglich.
Lesen (RX)	Ermöglicht den Zugriff im Umfang der Zugriffsart <i>Anzeigen</i> ; zusätzlich kann der Inhalt von Dateien gesichtet werden, Anwendungsprogramme können ausgeführt werden.
Hinzufügen (WX)	Unterverzeichnisse und Dateien können erstellt werden, der Zugriff auf bereits vorhandene Daten ist jedoch nicht möglich.
Hinzufügen und Lesen (RWX)	Kombination der Zugriffsarten <i>Hinzufügen</i> und <i>Lesen</i>
Ändern (RWXD)	Ermöglicht den Zugriff im Umfang der Zugriffsart <i>Hinzufügen und Lesen</i> ; zusätzlich können Dateien im Inhalt verändert oder gelöscht werden; Unterverzeichnisse können ebenfalls gelöscht werden.
Vollzugriff (Alle Rechte)	Ermöglicht den Zugriff im Umfang der Zugriffsart <i>Ändern</i> ; zusätzlich können Berechtigungen für Unterverzeichnisse und Dateien geändert und der Besitz dafür übernommen werden.
Besitz übernehmen (P)	Ermöglicht die Übernahme von Eigentumsrechten
Berechtigungen ändern (O)	Ermöglicht das Ändern von Berechtigungen

Die jeweiligen Zugriffsrechte werden über das Eigenschaftsfenster für jedes einzelne Verzeichnis oder jede einzelne Datei vergeben (vgl. Abb. 1).

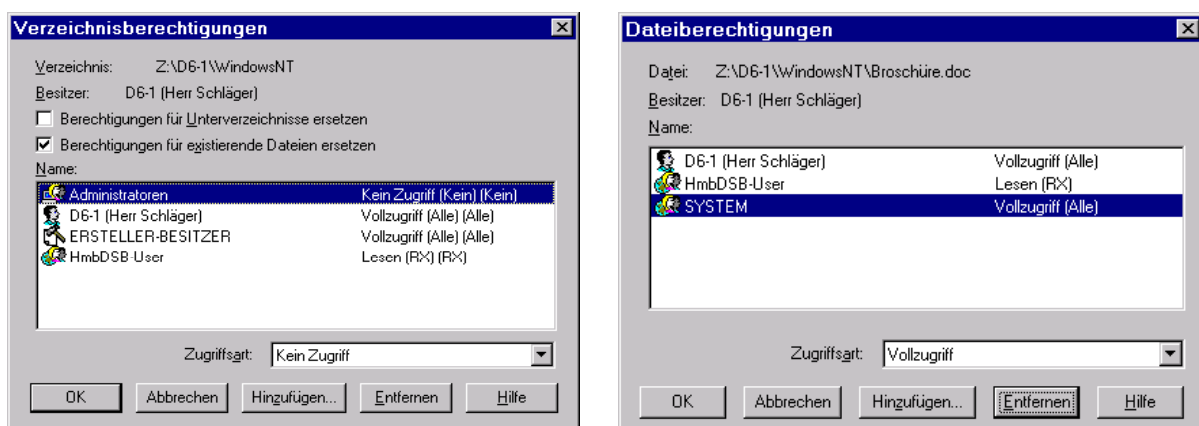


Abbildung 1: Verzeichnis- und Dateiberechtigungen

Zusätzlich führt das Dateisystem NTFS den Begriff des Besitzes an Dateien und Verzeichnissen ein. Besitzer einer Datei oder eines Verzeichnisses ist zunächst der Benutzer, der eine Datei oder ein Verzeichnis erstellt hat. Massgeblich ist dabei der Benutzername, unter dem sich ein Benutzer angemeldet hat. Durch das Besitzverhältnis erhält der Besitzer automatisch das Recht *Vollzugriff* an der Datei oder dem Verzeichnis. Er hat damit die Möglichkeit, Rechte an dieser

Datei zu vergeben, obwohl er nicht Administrator des Systems oder ein Benutzer mit besonderen Rechten ist.

Für Verzeichnisse und Dateien mit sensiblem Inhalt sollten dem Administrator die Zugriffsrechte entzogen werden. Er hat zwar in diesem Fall trotzdem die Möglichkeit, sich die Zugriffsrechte durch Besitzübernahme erneut zu gewähren. Dies kann jedoch nicht rückgängig gemacht werden und ist damit für den ursprünglichen Eigentümer der Datei zumindest nachvollziehbar (vgl. Kap. 7.5). Die Besitzübernahme an Dateien und Verzeichnissen ist über das Eigenschaftenfenster möglich.

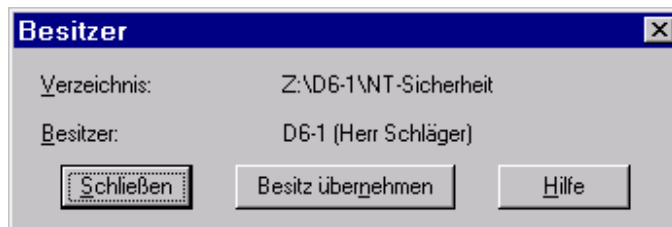


Abbildung 2: Besitzübernahme

8.2 Security Account Manager

Bei der Authentifizierung werden Benutzerkennung und Passwort verschlüsselt an den im User-Mode implementierten Security Account Manager (SAM) weitergeleitet, der die Eingaben bei der Anmeldung verifiziert. Nach erfolgreicher Anmeldung wird den Benutzern ein Berechtigungsausweis ausgestellt, der nicht nur die Zugriffsrechte des Benutzers festhält, sondern auch Auskunft darüber gibt, welchen Gruppen der Benutzer angehört. Systemintern wird anstelle der Benutzerkennung ein Sicherheits-Identifikator (SID) benutzt. Der Security Account Manager verwendet die in der Datei `winnt\system32\config\sam` gespeicherten Benutzerdaten. Der direkte Zugriff auf die SAM-Datei ist nicht möglich, da sie ständig vom Betriebssystem benutzt wird und somit immer geöffnet ist.

Aus Kompatibilitätsgründen weist die SAM-Datei zwei codierte Passwörter auf. Ein zum LAN-Manager kompatibles Passwort und eines für Windows NT. Das Passwort für den LAN-Manager besteht aus max. 14 Zeichen, während das Passwort für Windows NT bis zu 128 Zeichen lang sein kann.

Mittlerweile existieren zahlreiche Brute-Force-Programme, die an dem zum LAN-Manager kompatiblen Passwort ansetzen und die SAM-Datei in kurzer Zeit entschlüsseln können. Das Auslesen der SAM-Datei erfolgt entweder von einem anderen Betriebssystem aus oder wiederum durch entsprechende Hackertools wie beispielsweise *PWDump*, die die chiffrierten Passwörter aus der SAM-Datei extrahieren.

Standardmäßig existiert zudem noch eine Kopie der SAM-Datei (`Winnt\repair\SAM._`), die jeder lesen kann, der angemeldet ist. Um einen Brute-Force-Angriff zu erschweren, sollte die Kopie der SAM-Datei daher lediglich auf einer Diskette hinterlegt werden.

Um das Ermitteln von Passwörtern zu verhindern, steht ab dem Service Pack 3 das Programm *Syskey* zur Verfügung, das zusätzlich eine 128Bit-Verschlüsselung der SAM-Datei und deren Kopie ermöglicht. Von *Syskey* sollte daher in jedem Fall Gebrauch gemacht werden.

Passwörter können allerdings auch ohne Zugriff auf die SAM-Datei automatisiert ausprobiert werden, sofern die Anzahl der Login-Fehlversuche nicht begrenzt wird. Ein sehr effektives Programm zum Erraten von Passwörtern stellt NTCrack dar (s0marsoft.com/ftp/ntcrack.zip). NTCrack ist in der Lage, auch Domänenkonten zu attackieren und – je nach Kapazität des Netzwerks und des Servers – mehr als 1000 Loginversuche pro Minute zu starten.

NT sollte daher im Benutzer-Manager unter Richtlinien/Konten so konfiguriert werden, dass das Benutzerkonto nach mehr als 5 fehlerhaften Anmeldeversuchen gesperrt wird und die benutzten Passwörter mindestens 6 Zeichen lang sind. Passwörter sollten höchstens 90 Tage gültig sein. Neue Passwörter sollten mit den letzten 5 zurückliegenden Passwörtern verglichen werden (vgl. Abb. 3). Hierfür steht seit dem Service Pack 2 ein entsprechender Passwortfilter zur Verfügung, der in den Ordner `winnt\system32` kopiert und per Registry-Eintrag aktiviert wird.

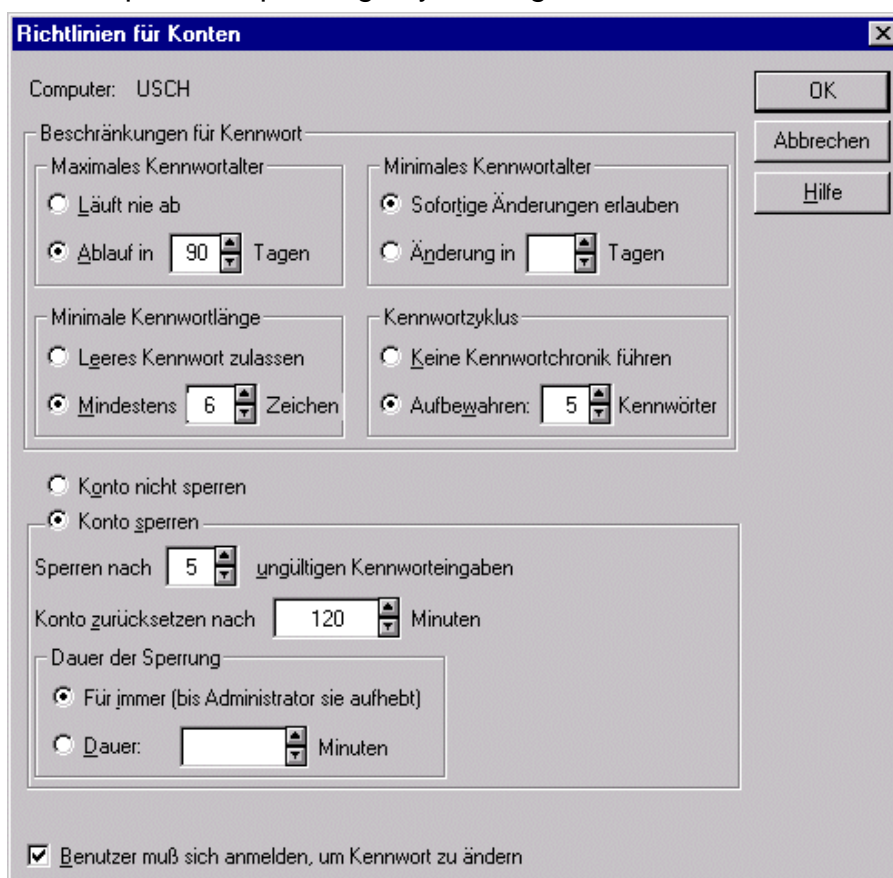


Abbildung 3: Passwort-Richtlinien im Benutzer-Manager

Die Begrenzung der Fehlversuche ist für die Systemverwalterkennung jedoch nicht möglich, um eine (böswillige) Sperrung dieses Kontos zu verhindern. Um unberechtigte Anmeldeversuche unter der Administratorkennung zu erschweren, sollte diese Kennung daher zum einen umbenannt werden. Zum anderen sollte die Anmeldung nur am Server selbst oder an ausgewählten Workstations möglich sein.

Die Änderung der Standardeinstellungen auf die empfohlenen Einstellungen wird jedoch nur für Benutzer wirksam, die nach der Änderung neu aufgenommen werden. Benutzerkonten, die vor der Standardfestlegung eingerichtet wurden, sind nachträglich einzeln anzupassen.

8.3 Registry

Der Zugriff auf Disketten- oder CDROM-Laufwerke, auf Programme und andere NT-Ressourcen werden systemseitig in der Registry ebenso verwaltet wie Sicherheitseinstellungen, die der Internet Explorer nutzt. Somit hat die Registry hinsichtlich der Datensicherheit einen hohen Stellenwert.

Ordnungsgemäß angemeldete Benutzer sind jedoch automatisch Mitglied der Gruppe *Jeder*, deren Mitglieder standardmäßig begrenzt auf bestimmte Registry-Teilschlüssel zugreifen dürfen. Dies gilt auch für Trojanische Pferde, die in der Benutzerumgebung zur Ausführung gelangen.

Um das Verändern von Registryeinträgen durch den Benutzer bzw. unter seiner Kennung agierenden Programmen zu verhindern, sollten die Benutzer auf sicherheitskritische Teilschlüssel der Registry nur lesend zugreifen dürfen (z.B. sämtliche Teilschlüssel von HKEY_CLASSES_ROOT, sämtliche Teilschlüssel von HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RPC, Teilschlüssel von HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurentVersion). Dies erfolgt mit Hilfe des Registry-Editors *regedt32* unter *Sicherheit/Berechtigungen*.

Es ist grundsätzlich empfehlenswert, den Zugriff der Anwender auf die Registry-Editoren zu unterbinden und *regedt32.exe* und *regedit.exe* zu deinstallieren bzw. den Zugriff hierauf durch den Systemrichtlinien-Editor einzuschränken. Der Zugriff des Systemverwalters auf die Registry erfolgt stattdessen remote über Editoren, die auf dem Server hinterlegt und dort vor missbräuchlichem Zugriff geschützt sind. Ein Deaktivieren bzw. Sperren der Registry-Editoren ist jedoch nicht so wirksam wie das aufwändigere Einschränken der Zugriffsrechte, da es möglich ist, auch ohne Nutzung der genannten Editoren die Registry zu lesen und zu verändern.

8.4 Protokollierung

Windows NT bietet standardmäßige Funktionen zur Protokollierung von System-, Anwendungs- und Benutzeraktivitäten. Festgelegte oder auswählbare Ereignisse werden in drei Bereichen protokolliert:

- Das Systemprotokoll enthält die Ereignisse aller internen Windows NT-Dienste und -Treiber. Es kann daher ggf. festgestellt werden, ob unbekannte Treiber oder Dienste installiert worden sind.
- Das Anwendungsprotokoll enthält Ereignisse, die von Anwendungen erzeugt werden. So kann beispielsweise ein Datenbankprogramm einen Dateifehler im Anwendungsprotokoll aufzeichnen. Die Nutzung des Protokolls ist von der Anwendung abhängig, d. h. die Anwendung muss die Protokollierung anstossen. Bei selbst entwickelten Anwendungen können beliebige Protokolleinträge erzeugt werden.
- Im Sicherheitsprotokoll werden alle Ereignisse notiert, die in den Überwachungsrichtlinien des Systems festgelegt wurden.

Es wird empfohlen, die Protokollierung folgender Ereignisse festzulegen (vgl. Abb. 4):

- fehlerhaftes An- und Abmelden (wird eingestellt in den Überwachungsrichtlinien im Benutzer-Manager),
- fehlerhafte Dateizugriffe (Überwachungsrichtlinieneditor),
- fehlerhafte Verwendung von Benutzerrechten (Überwachungsrichtlinieneditor),
- erfolgreiche und fehlerhafte Aktivitäten der Benutzer- und Gruppenverwaltung (Überwachungsrichtlinieneditor),
- erfolgreiche und fehlerhafte Änderungen der Sicherheitsrichtlinien (Überwachungsrichtlinieneditor),
- erfolgreiches und fehlerhaftes Neustarten und Herunterfahren des Servers (Überwachungsrichtlinieneditor),
- sämtliche Remote-Zugriffe (hierzu muss in der Registry das Feld Enable Audit im Teilschlüssel *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters* auf 1 gesetzt werden)
- Zugriffe auf die Server-Registry (wird eingestellt in der Registrierungsschlüsselüberwachung),
- Zugriffe auf Unterverzeichnisse bzw. Dateien, in denen sensible Dokumente gespeichert sind (wird eingestellt in den Unterverzeichnis- bzw. Datei-Eigenschaften).

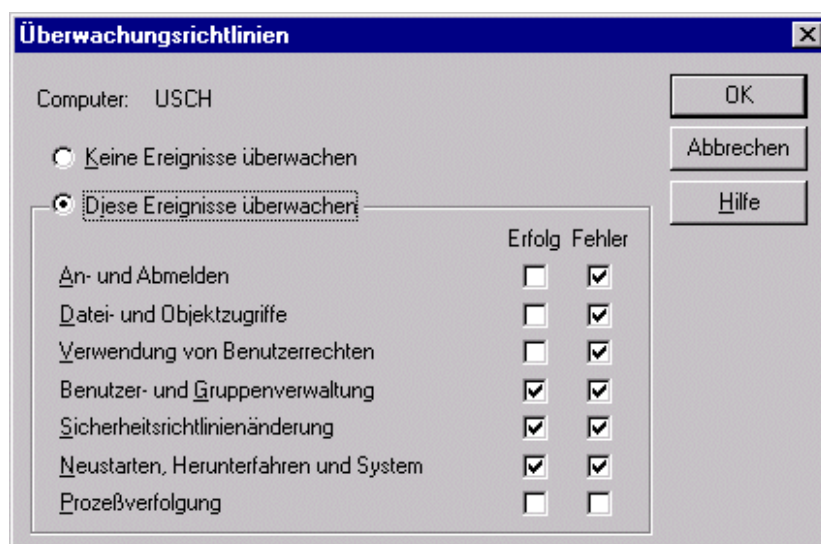


Abbildung 4: Festlegung der Protokollierung in Überwachungsrichtlinien

Die Protokolle sollten über die aufgeführten sicherheitsrelevanten Systemaktivitäten mindestens 14 Tage rückwirkend Auskunft geben können. Die Protokolle sollten stichprobenartig sowie bei konkreten Anlässen ausgewertet werden. Hierzu kann das Gesamtprotokoll nach bestimmten Ereignissen gefiltert werden. Sicherheitsrelevante Ereignisse mit hoher Priorität können zudem eine sofortige Reaktion des Systems veranlassen (z.B. eine Benachrichtigung des Systemverwalters). Die Auswer-

tung sollte möglichst arbeitsteilig unter einer eigens hierfür vorgesehenen Revisorenkennung erfolgen.

Der Systemverwalter selbst lässt sich durch die Protokolldateien allerdings nur begrenzt kontrollieren, da die Protokolldateien weder verschlüsselt gespeichert werden noch dem Vier-Augen-Prinzip unterliegen. Er kann jederzeit sämtliche Protokolldateien löschen.

8.5 Rechte des Systemverwalters

Zugriffsrechte auf Dateien und Verzeichnisse können bei Windows NT sowohl vom Systemverwalter als auch vom Eigentümer der Objekte vergeben werden. Dies bedeutet, dass der Eigentümer auch dem Systemadministrator den Zugriff auf eigene Dateien verwehren kann. Standardmäßig kann der Administrator einer NT-Domäne sämtliche Daten lesen und verändern sowie in die Zugriffsmechanismen des Betriebssystems eingreifen. Es wird empfohlen, dass sich der Administrator Zugriffsrechte auf sensible Dateien bzw. Unterverzeichnisse selbst entzieht oder ihm diese Rechte vom Eigentümer der jeweiligen Home-Verzeichnisses entzogen werden. Zwar kann sich der Administrator die Rechte auch selbst wieder zuteilen, indem er zunächst Eigentümer des Unterverzeichnisses bzw. der Dateien wird. Da die Besitzübernahme jedoch vom Administrator nicht rückgängig gemacht werden kann, ist ein Zugriff auf fremde geschützte Dateien zumindest nachträglich erkennbar.

Windows NT verfügt zudem über die Möglichkeit, administrative Aufgaben auf mehrere Sub-Systemverwalter mit eingeschränkten Administrationsrechten zu verteilen.

Administrative Aufgaben sollten auf folgende Systemverwalter verteilt werden:

- Der Domänen-Administrator definiert Benutzergruppen, richtet neue Benutzer ein und ist für die Vergabe neuer Passwörter zuständig. Er hat alleiniges Zugriffsrecht auf den Systemrichtlinieneditor. Hierüber wird domänenweit die Arbeitsumgebung einschließlich der lokal ausführbaren Programme für sämtliche Benutzergruppen festgelegt.
- Zusätzliche Abteilungsadministratoren sind Eigentümer von sämtlichen Dateien und Verzeichnissen, auf die von Mitarbeitern der jeweiligen Abteilung zugegriffen wird, und können dem Domänen-Administrator die Zugriffsrechte entziehen.
- Sicherungs- und Replikations-Operatoren werden von Windows NT bereits standardmäßig zur Verfügung gestellt.
- Revisoren sollten auf die Ereignisanzeige zugreifen. Den übrigen Benutzern sind die Zugriffsrechte auf die Protokolldateien (`\\Winnt\system32*.log`) entsprechend einzuschränken.

In kleineren Organisationseinheiten können mehrere Rollen auch von einer Person wahrgenommen werden. Die Auswertung von Systemprotokollen unter der Revisorenkennung sollte möglichst einer Person übertragen werden, die nicht die Systemverwaltung wahrnimmt.

Um den Zugriff von Systemadministratoren auf sensible Dateien vollständig auszuschließen, sollte den Benutzern die Möglichkeit gegeben werden, die Daten bei Bedarf zu verschlüsseln. Hierfür und zum Versenden vertraulicher elektronischer Post über das Internet wird der Einsatz geeigneter Verschlüsselungsprogramme wie beispielsweise Pretty Good Privacy (PGP) empfohlen.

Darüber hinaus sollten nicht benötigte Benutzerkennungen im Benutzer-Manager gelöscht werden. Da dies bei der Standard-Kennung *Gast* nicht möglich ist, sollte die *Gast*-Kennung deaktiviert werden. Ebenso sollten Posix- und OS/2-Subsysteme – sofern sie nicht für 16-Bit- bzw. OS/2-Anwendungen benötigt

werden – gelöscht werden, da beide Subsysteme sicherheitskritische Funktionen enthalten können. Dies erfolgt durch Löschen des entsprechenden Eintrags im Registry-Schlüssel `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\Subsystems`.

Zugriffsrechte auf ausgewählte NT-Objekte können domänenweit durch Einsatz des Systemrichtlinieneditors vergeben werden, beispielsweise der Zugriff auf Registry-Editoren, das Deaktivieren der Ausführen-Funktion in der Start-Leiste. Hiervon sollte Gebrauch gemacht werden.

Die Administratorkennung sollte nicht netzweit, sondern nur von einem Arbeitsplatz-PC aus aufgerufen werden. Dies lässt sich im Benutzermanager unter *Benutzereigenschaften* einstellen. Auch die Kennungen, mit denen auf personenbezogene Dokumente zugegriffen wird, sollten im Benutzermanager auf gleiche Weise arbeitsplatzbezogen vergeben werden.

9 NT-Systeme als Bestandteil heterogener Netze

Während in Kapitel 6 bereits die grundlegenden Aspekte von NT-Client-Server-Netzen erörtert wurden, werden in diesem Kapitel Anforderungen formuliert, die beim Anschluss eines NT-Systems an andere Netze wie z.B. das Internet oder bei der Einrichtung von Einwählverbindungen zu beachten sind.

9.1 Remote Access Service (RAS)

Mittels des RAS-Dienstes ist ein Fernzugriff auf NT-Systeme (Workstation und Server) möglich, um beispielsweise einen Filialstandort anzubinden oder Mitarbeiter zu ermöglichen, von unterwegs aus mittels Modem auf das Firmennetz zuzugreifen. Benutzer, die über RAS auf einem NT-System angemeldet sind, unterliegen den gewöhnlichen NT-Schutzmechanismen hinsichtlich Zugriffsrechten und Protokollierung.

Um den unberechtigten Zugriff mittels RAS zu verhindern, bietet dieser Dienst eine Reihe von Sicherheitsmerkmalen. Für einen sicheren Betrieb eines RAS-Servers werden insgesamt folgende Maßnahmen vorgeschlagen:

- Die Authentisierung der RAS-Benutzer sollte über das Protokoll CHAP (Challenge Handshake Authentication Protocol) erfolgen. Beim CHAP-Verfahren wird vom RAS-Server nach dem Verbindungsaufbau ein Zufallscode generiert. Dieser wird zum Anrufenden übertragen, dort mit dem Passwort verschlüsselt und zum Angerufenen zurückübermittelt. Der RAS-Server entschlüsselt den übermittelten Wert wieder und vergleicht ihn mit dem Ausgangswert. Stimmen sie überein, gilt der RAS-Benutzer als authentisiert. Das CHAP-Verfahren sieht außerdem eine regelmäßige Authentisierung während einer bestehenden Verbindung vor. Nach einem erfolgreichen Verbindungsaufbau wird das Passwort kontinuierlich von neuem angefordert. Zudem bietet das CHAP-Verfahren die Möglichkeit, auch die Inhaltsdaten verschlüsselt zu übertragen. Die Verschlüsselung erfolgt hierbei entweder nach dem DES- oder – sofern dies von Client-Seite unterstützt wird – nach dem RC4-Verfahren. Aufgrund der Challenge-Response-Prozedur ist das CHAP-Verfahren jedoch nur dann benutzbar, wenn auch der Kommunikationspartner CHAP-Funktionalität besitzt.

Dazu ist in den Eigenschaften des RAS-Dienstes unter *Netzwerk/Server-Einstellungen* die Option *Nur Microsoft-verschlüsselte Echtheitsbestätigung* zu aktivieren sowie – für die Inhaltsverschlüsselung – das Feld *Datenverschlüsselung fordern* (siehe Abb.5).

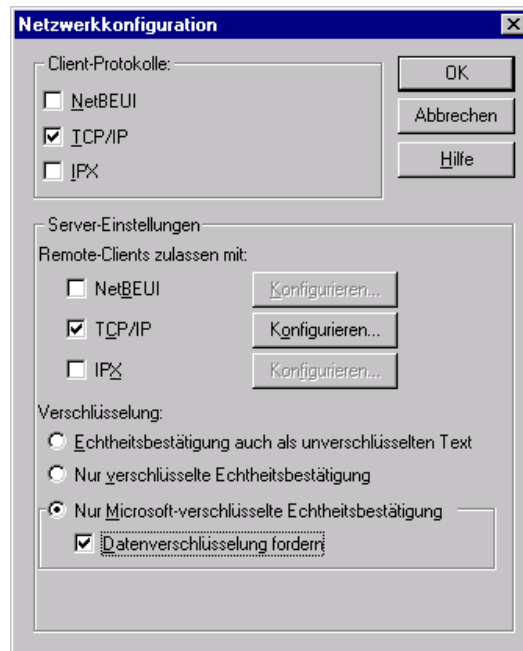


Abbildung 5: Datenverschlüsselung

- Nur diejenigen Benutzer sollten für die Benutzung des RAS-Dienstes freigeschaltet werden, die diesen benötigen. Für Benutzer mit festem Standort sollte die Rückruf-Option aktiviert werden, so dass die Verbindung nicht von einem anderen Standort aus aufgebaut werden kann. Dies erschwert eine unberechtigte Anmeldung erheblich.

Dazu ist in der RAS-Verwaltung unter *Benutzer*, *Remote-Zugriffsberechtigungen* nur für die jeweils berechtigten Benutzer das Feld *Dem Benutzer RAS-Zugriffsrechte erteilen* zu aktivieren sowie unter *Rückruf* im Feld *Vorbelegung* die Anschlussnummer des Endgerätes für den Rückruf einzutragen (siehe Abb. 6).

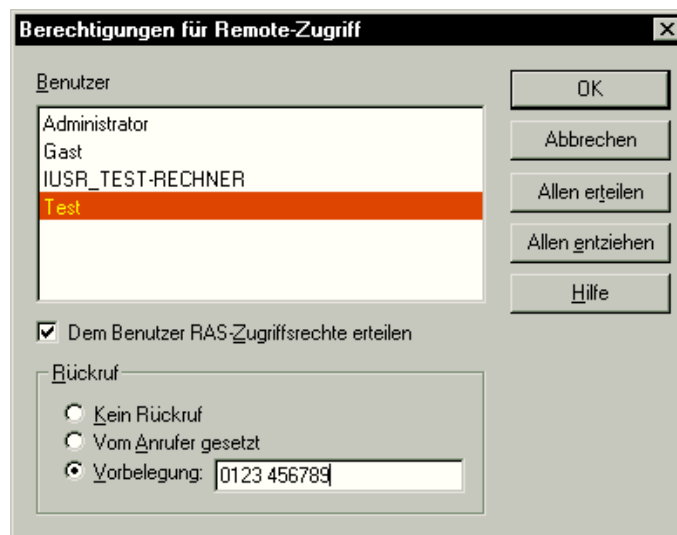


Abbildung 6: Berechtigungen für Zugriff auf RAS-Server

- Möglichst ist der Zugriff von RAS-Clients auf den RAS-Server zu begrenzen und ein Zugriff auf andere Rechner im lokalen Netzwerk zu verhindern.

Dazu ist in den Eigenschaften des RAS-Dienstes unter *Netzwerk/Konfigurieren* für jedes zugelassene Protokoll (TCP/IP, IPX oder NetBEUI) in der Auswahl *Clients dürfen zugreifen auf:* das Feld *Nur diesen Compute* zu aktivieren (siehe Abb. 7).

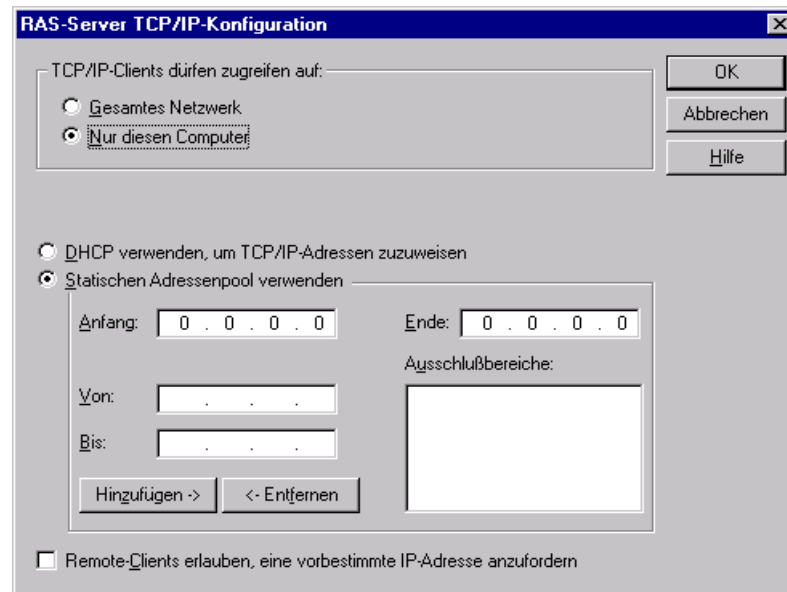


Abbildung 7: Begrenzung des Remote-Zugriffs auf einzelne Arbeitsplätze

- Sämtliche Remote-Zugriffe sollten protokolliert werden. Hierzu muss in der Registry das Feld *Enable Audit* im Teilschlüssel *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters* auf 1 gesetzt werden.
- Für Systemverwalterkennungen und Kennungen mit Zugriff auf sensible personenbezogene Daten sollte kein Remote-Zugriff eingerichtet werden. Die damit verbundenen Risiken sind auch bei optimalen Einstellungen des RAS-Dienstes als zu hoch einzustufen.

9.2 Internetanschluss

Wird ein NT-System direkt oder über ein lokales Netzwerk an das Internet angeschlossen, entstehen zusätzliche Risiken. Dabei sind im Wesentlichen drei Gefahrenpotentiale erkennbar:

1. Aus dem Internet erfolgt ohne Zutun des Benutzers ein Zugriff auf das NT-System mittels der darauf eingerichteten Netzwerkdienste.
2. Der Benutzer versendet (personenbezogene) Daten ins Internet und unterläuft dadurch lokal wirkende Beschränkungen des Datenexports.
3. Der Benutzer lädt Software aus dem Internet, ohne die Qualität und den Hersteller der Software genauer zu kennen. Die Software kann verdeckte Funktionen bzw. Viren und Trojanische Pferde etc. enthalten, die nicht nur den lokalen Betrieb stören, sondern über den Internetanschluss selbstständig Daten aus dem System versenden.

Dem Risiko, dass aus dem Internet auf das NT-System zugegriffen wird, kann dadurch begegnet werden, dass keine (unnötigen) Netzwerkdienste eingerichtet werden. NT-Workstations sollten keinerlei Server-Funktion anbieten; NT-Server sollten nur die für den Server-Betrieb erforderlichen Dienste zur Verfügung stellen (aktive TCP/IP-Netzwerkdienste können in der NT-Shell mit *netstat -a* angezeigt werden).

Besonderes Augenmerk sollte dabei den sog. NetBIOS-Ports (insbes. Port 139) gelten. Über diese Ports sind freigegebene Dateien und Verzeichnisse sowie sonstige NT-Ressourcen mittels TCP/IP erreichbar. Dabei kann die Maßnahme, einen unberech-

tigten Zugriff von aussen durch die Vergabe von Kennwörtern zu verhindern, durch den Einsatz von Passwortgeneratoren unter Umständen erfolgreich unterlaufen werden. Angesichts der Risiken, die von den NetBIOS-Ports ausgehen, sollten diese Ports erst gar nicht aus dem Internet erreichbar sein. Dies ist mit ausreichendem Schutzniveau letztlich nur durch den Betrieb einer Firewall sicherzustellen; zu dieser Thematik gibt die "Orientierungshilfe Internet" des Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder weitere Hinweise.

Die beiden anderen Risiken (unbefugter Versand personenbezogener Daten und Einschleppen von Viren) können durch den Einsatz einer Firewall jedoch nicht effektiv unterbunden werden, da sich diese Risiken von einer rechtmäßigen Nutzung der Dienste technisch kaum unterscheiden lassen. Effektiver

Schutz kann durch getrennte Arbeitsumgebungen für jeden Anwender erzielt werden. In der sog. Produktionsumgebung wird auf Client-Server-Anwendungen einschließlich Bürokommunikation zugegriffen, während die Transportumgebung für den Internetzugang und EMail sowie für den Dateitransfer per Diskette oder andere Medien zur Verfügung steht.

Die beiden Umgebungen werden durch die Einrichtung von zwei verschiedenen NT-Benutzern abgebildet, die verschiedene Rechte im lokalen System und auf den Dateiservern besitzen. Der Anwender wechselt je nach Erforderlichkeit zwischen den beiden Umgebungen, indem er sich beim Betriebssystem ab- und wieder anmeldet; ein Neustart des Systems ist dafür nicht erforderlich.

Während der Benutzer in der Produktionsumgebung Zugriff auf personenbezogene Daten besitzt, wird ihm dies in der Transportumgebung durch entsprechende NT-Zugriffsschutzeinstellungen verwehrt. Die Überwindung dieser Schutzmechanismen setzt die Kenntnis des Passworts für die Produktionsumgebung voraus. Dies können eventuelle Angreifer(programme) jedoch in der Transportumgebung nicht in Erfahrung bringen, sofern es sich von dem dort benutzten Kennwort hinreichend unterscheidet. Dateien, die aus dem Internet geladen oder als E-Mail-Anhänge empfangen werden, können daher in der Transportumgebung geöffnet bzw. ausgeführt werden, ohne dass hierdurch die personenbezogenen Daten der Produktionsumgebung gefährdet sind. Ausführbare Programme sollten nur in Ausnahmefällen nach ausgiebigem (Viren-)Test von der Transport- in die Produktionsumgebung übertragen werden.

Der Dateitransport zwischen den Umgebungen erfolgt über ein dafür eingerichtetes Verzeichnis, auf das von beiden Umgebungen aus lesend und schreibend zugegriffen werden kann. Indem die Dateibewegungen in diesem Verzeichnis protokolliert werden, kann der missbräuchliche Export sensibler Daten nachvollzogen werden. Letztlich entscheidet der Anwender jedoch eigenverantwortlich, welche Dateien zwischen den beiden Umgebungen ausgetauscht werden.

Zusätzlich zu den beiden Arbeitsumgebungen ist es notwendig, dass die für E-Mail- und Web-Zugriff benötigten TCP/IP-Ports entweder durch die Firewall oder andere Geräte benutzerbezogen gefiltert bzw. aktiviert werden. Eine Filterung allein der IP-Adresse ist nicht ausreichend, da die entsprechenden TCP/IP-Dienste auch in der Produktionsumgebung aufgerufen werden können. Die benutzerbezogene Filterung des E-Mail-Dienstes kann realisiert werden, wenn die elektronische Post nicht direkt (über Port 25) ins Internet verschickt werden kann, sondern nur über interne Mail-Server. Wenn auf den Mail-Servern nur ein Postfach für den Benutzer der Transportumgebung eingerichtet wird, kann aus der Produktionsumgebung heraus keine elektronische Post über den Mail-Server ins Internet verschickt werden.

Ähnliche Mechanismen können auch für den Web-Zugriff implementiert werden. Sofern über einen Proxy-Server auf das Internet zugegriffen wird, sollten möglichst nur solche Proxies eingesetzt werden, die den Internetzugriff nach vorheriger Authentisierung freigeben. Lässt sich der Proxy-Server in eine NT-Domäne einbinden, kann der Benutzer auch ohne zusätzliche Passwort-eingabe durch Abgleich mit dem PDC authentisiert werden. Eine derartige benutzerbezogene Freigabe des Web-Zugriffs hat den Vorteil, dass aus der Produktionsumgebung heraus keine Daten über die ansonsten für den gesamten Rechner freigegeben Ports (z.B. http und ftp) verschickt werden können.

9.3 Systems Management Server (SMS)

Der Systems Management Server ermöglicht die Verwaltung räumlich verteilter Windows-basierter Rechner von einer zentralen Stelle aus. Durch seine Architektur kann man in Netzen jeder Größenordnung, die aus diversen Domänen bestehen können, alle Aufgaben einer zentralen PC-Administration erledigen. Die wichtigsten Funktionen von SMS sind

- Aufbau und Pflege eines Bestands von Rechner-Hardware und -Software,
- Verteilung, Installation und Konfiguration von Software-Paketen,
- Fernsteuerung von anderen NT-Maschinen.

Da alle genannten Funktionen sicherheitskritisch sind und sich zudem auf ganze Netzwerke erstrecken können, kommt der Rechtevergabe bei SMS wesentliche Bedeutung zu. Da die Zugriffsrechte von SMS durch eine SQL-Server-Datenbank abgebildet werden, kann derjenige Datenbankadministrator, der Zugriff auf die SMS-Datenbank und deren Tabellen hat, Einfluss darauf nehmen, wer die verschiedenen administrativen Funktionen des SMS anwenden darf. Um eine Vermischung von regulärer Datenbank- und davon unabhängiger SMS-Verwaltung zu vermeiden, sollte die SMS-Datenbank von möglicherweise anderen installierten Datenbanken getrennt bzw. auf einem eigenen SQL-Server eingerichtet werden.

Die Zugriffsrechte auf SMS-Dienste können mit Hilfe des SMS Security Managers vergeben werden. Um die Rechtevergabe für SMS-Administratoren zu vereinfachen, sind einige vordefinierte Standardrollen entwickelt worden, auf die zunächst zurückgegriffen werden kann. Dennoch sollten die Zugriffsrechte der SMS-Benutzer an die konkreten Einsatzbedingungen vor Ort angepasst werden, um die unbefugte Benutzung von SMS-Funktionen auszuschließen.

Kritisch ist die Installation von Softwarepaketen mittels SMS, da die zu installierende Software (im Ordner SMS_PKGC) vor der Verteilung manipuliert werden kann. Zudem kann ein SMS-Administrator in den Paketen Skripte implementieren, die beliebige Funktionen auf dem Client aktivieren. Um dies auszuschließen, sollte (bei einer entsprechenden administrativen Arbeitsteilung) zum einen der entsprechende Ordner für den Software-Installierer gesperrt sein, zum anderen sollte die Erstellung von Installationspaketen nur von unveränderten Originalversionen erfolgen können.

Problematisch sind zudem die Remote-Dienste des SMS. Sofern die Programme des Package-Control-Managers (PCM) *PCMSVC32.EXE* und *PCMWIN32.EXE* auf einem Client installiert sind, ist ein Remote-Zugriff möglich, auch ohne dass ein Benutzer angemeldet ist. Mit Hilfe dieses Dienstes können beispielsweise Dateien auch in gesicherten Ordnern installiert oder Registry-Schlüssel geändert werden, falls ein Benutzerkonto mit Administratorrechten auf dem jeweiligen Rechner eingerichtet ist und die entsprechenden SMS-Rechte vorhanden sind. Domänen-Administratoren sowie Benutzer mit lokalen Administrationsbefugnissen haben standardmäßig solche Rechte; diese sollten daher entsprechend eingeschränkt werden. Sofern der PCM-Dienst nicht benötigt wird, sollte er vollständig von den Clients entfernt bzw. erst gar nicht installiert werden.

Bei den standardisierten Remote-Operationen kann ein Missbrauch hingegen bereits durch den Benutzer verhindert werden. Mit den HelpDesk-Optionen können vor Ort einzelne Remote-Zugriffsarten aktiviert bzw. deaktiviert werden. Bei aktivierter Funktion werden der Zugriffswunsch des anfragenden Rechners incl. des Netzwerknamens des dort angemeldeten SMS-Administrators übermittelt und eine Erlaubnis des lokalen Benutzers eingeholt. Darüber hinaus hat der Benutzer ständige Kontrolle über

die Aktivitäten des Administrators und kann die Remote-Operation jederzeit abbrechen, sofern er in den notwendigen Rechten zum Beenden von Prozessen nicht eingeschränkt wurde (siehe Abb. 8 und 9).

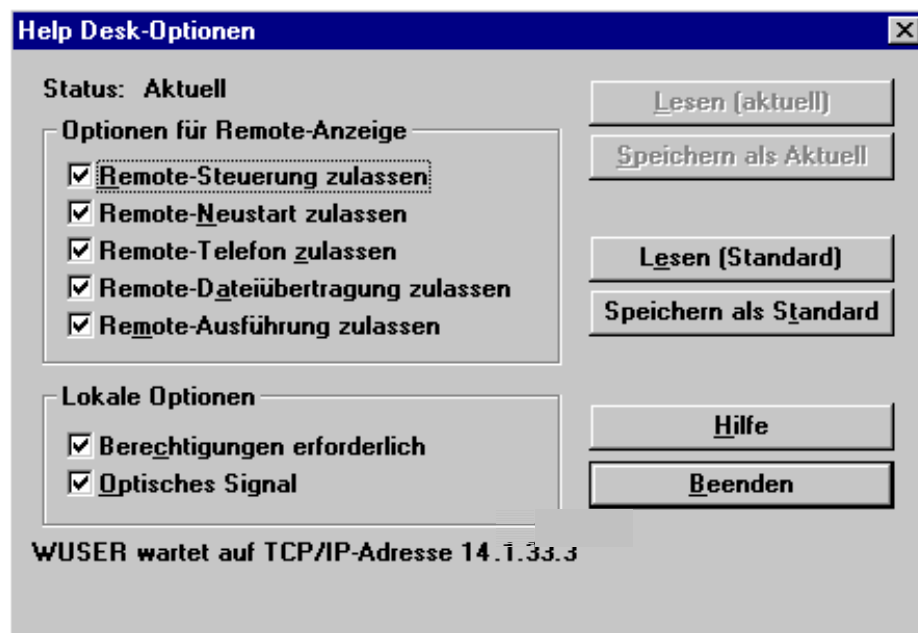


Abbildung 8: Einstellung der Help-Desk-Optionen

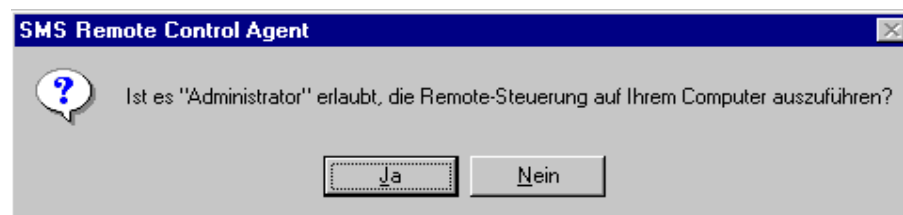


Abbildung 9: Information des Benutzers während des Remote-Zugriffs

10 Sicherheitsrelevante Neuerungen von Windows 2000

Die Aussagen dieses Kapitels basieren auf Informationen zu Windows 2000 Beta 3. Es können sich daher Änderungen zu dem ausgelieferten Produkt ergeben, die bei Drucklegung nicht vorhersehbar waren. Allerdings haben wir uns bemüht, nur solche grundlegenden Aspekte zu behandeln, die nach aller Wahrscheinlichkeit auch im endgültigen Release Bestand haben werden.

10.1 Windows 2000 und Windows NT

Windows 2000 ist als Weiterentwicklung von Windows NT 4.0 konzipiert und somit für den professionellen Einsatz vorgesehen. Obwohl Elemente der Produktlinie von Windows 95/98 in die neue Version eingeflossen sind, wird Windows 95/98 für den Privatbereich weiter angeboten.

Insgesamt sind drei verschiedene Windows-2000-Produkte vorgesehen. Professional entspricht der Workstation-Variante von NT4, (Advanced) Server dem bisherigen NT-Server (Enterprise Edition), und DataCenter Server ist eine erweiterte Serverversion für hochperformante Anwendungen.

Neben einer Reihe von Funktionserweiterungen gegenüber Windows NT 4.0 sowie Maßnahmen, die die Stabilität erhöhen sollen, wurden auch in Hinblick auf die Sicherheit Neuerungen vorgenommen. Im Folgenden sind zunächst die wesentlichen Erweiterungen aufgeführt. Wann ein Wechsel auf Windows 2000 aus Sicherheitsgründen empfehlenswert erscheint, wird abschließend diskutiert.

10.2 Encrypting File System (EFS)

Erstmals wird in Windows 2000 in einem kommerziellen Betriebssystem standardmäßig die Möglichkeit angeboten, Dateien transparent zu verschlüsseln. Diese Funktionalität war bislang Zusatzprodukten vorbehalten und erforderte somit einen zusätzlichen finanziellen und administrativen Aufwand. Die datenschutzrechtliche Forderung nach Vertraulichkeit von gespeicherten Daten auch bei direktem Zugriff auf die Festplatte (z.B. bei Diebstahl eines Laptops oder im Rahmen der Wartung) kann mittels Windows 2000 daher effektiver umgesetzt werden.

Das EFS ist eng an das Dateisystem NTFS angebunden und arbeitet für den Benutzer weitgehend transparent, nachdem die erforderlichen Einstellungen vorgenommen worden sind. Diese bestehen neben der einmaligen Schlüsselgenerierung im Wesentlichen daraus, auf Verzeichnisebene festzulegen, welche Daten verschlüsselt werden sollen. In entsprechend markierten Verzeichnissen wird dann die Ver- und Entschlüsselung sämtlicher Dateien und Unterverzeichnisse automatisch vorgenommen. Einschränkungen bestehen allerdings zurzeit hinsichtlich der Möglichkeit, verschlüsselte Dateien mehreren Benutzern zugänglich zu machen sowie die Verschlüsselung auf einzelne Dateien zu begrenzen. Diese Möglichkeiten sollen später ergänzt werden.

Als Kryptoalgorithmus wird DESX (DES Extended, eine Erweiterung des DES-Algorithmus, um sog. Brute-Force-Attacken zu erschweren) verwendet, wobei innerhalb der USA die volle maximale Schlüssellänge von 120 Bit, außerhalb jedoch – aufgrund US-amerikanischer Exportbestimmungen – nur 40 Bit angeboten werden.

Integraler und nicht abschaltbarer Bestandteil des EFS ist die Möglichkeit, Dateien auch ohne den privaten Schlüssel des Benutzers zu entschlüsseln (Data Recovery). Standardmäßig besitzt der Domänenadministrator oder in domänenlosen Installationen der lokale Administrator dieses Recht bzw. verfügt über den Recovery-Schlüssel. Eine Verschlüsselung im Namen des Benutzers ist damit nicht möglich.

Ein weiteres Element, um Datenverlust im Rahmen der Verschlüsselung vorzubeugen, ist das Crash Recovery. Während jedes Ver- oder Entschlüsselungsvorgangs wird die betreffende Datei temporär im Klartext gespeichert, bis die Operation erfolgreich beendet wurde; dann wird die Kopie gelöscht. Wird die Operation vorzeitig beendet (z.B. durch einen Stromausfall), kann auf die Kopie noch zugegriffen werden. Dabei entstehen allerdings auf der Festplatte Kopien der zu schützenden Daten im Klartext, die erst im Rahmen der Wiederverwendung von Speicherblöcken endgültig überschrieben werden. Systemdateien, die erst beim Systemstart benötigt werden, werden jedoch nicht von EFS erfasst, da die Ver- und Entschlüsselung erst nach dem Laden des Betriebssystems verfügbar ist.

10.3 Zugriffsrechte

Hinsichtlich der Zugriffsschutzmechanismen bietet Windows 2000 keine Erweiterungen gegenüber Windows NT bei Verwendung des NTFS-Dateisystems. Aller-

dings werden die vorhandenen Möglichkeiten durch eine erweiterte Definition von Standardrollen besser genutzt. In Windows 2000 werden drei Klassen von Benutzern unterschieden: Administratoren, Benutzer (Power-User) und Anwender (User). Dabei ist die Administrator-Klasse mit der von Windows NT identisch, während der Benutzer dem gewöhnlichen Windows-NT-Benutzer entspricht, der zwar nicht über Administrationsrechte verfügt, jedoch weitgehende Manipulationen im System vornehmen kann. Neu ist die Rolle des Anwenders, der keine Änderungen an Verzeichnissen oder in der Registry vornehmen kann, die sich auf andere Benutzer auswirken. Damit soll vermieden werden, dass sich verschiedene Benutzer eines Windows-Systems gegenseitig stören, beispielsweise wenn im Rahmen von Installationsvorgängen DLL-Dateien im Systemverzeichnis oder übergreifende Registryeinträge verändert werden. Insbesondere die Einbeziehung der Registry in die Zugriffsbeschränkungen eines Anwenders macht dieses neue Konzept interessant. Die bereits in Windows NT bestehende, aber selten eingesetzte Möglichkeiten, Teile der Registry gegen Veränderung und damit das System insgesamt zu schützen, kann dadurch ohne großen Aufwand genutzt werden.

Der durchgängigen Verwendung der Anwender-Rolle für die gewöhnliche Nutzung steht allerdings entgegen, dass viele Anwendungsprogramme mit den eingeschränkten Zugriffsrechten nicht auskommen und insofern zunächst auf Windows 2000 umgestellt werden müssen. Aus diesem Grund werden die Standardrollen von Windows 2000 nur bei einer Neuinstallation, nicht aber bei einer Installation über Windows NT eingerichtet. In diesem Fall müssen die Zugriffsrechte explizit gesetzt werden. Bei den genannten Benutzerklassen handelt es sich um Standardwerte, die bei Bedarf den jeweiligen Erforderlichkeiten angepasst oder durch weitere Differenzierungen ergänzt werden können.

10.4 Kerberos

Eine weitere Neuerung von Windows 2000 betrifft die Authentisierungsmechanismen bei der Anmeldung in einer Domäne. Während Windows NT dafür das Windows-NT-LAN-Manager-Protokoll (NTLM) verwendet, basiert Windows 2000 auf Kerberos 5. Dies bringt eine Reihe von Vorteilen mit sich.

Authentisierungen sind damit beidseitig möglich; nicht nur ein Server kann die Identität eines Clients überprüfen (wie bereits mit NTLM), sondern auch umgekehrt ein Client die Identität eines Servers. Dabei basiert die Überprüfung nicht auf der Verbindung zu einem Domain-Controller, so dass die Notwendigkeit entfällt, in Multidomänenumgebungen komplexe Vertrauensbeziehungen zwischen Domain-Controllern einzurichten. Schließlich findet mit Kerberos ein außerhalb von Microsoft entwickelter, bewährter Standard Verwendung, dessen Qualität (unabhängig von eventuellen Implementationsdefiziten) ausreichend validiert ist. Die Verwendung von Kerberos ist auch in gemischten Windows-Netzen möglich, wobei nur dann auf NTLM zurückgegriffen wird, wenn auf einem der beteiligten Geräte kein Windows 2000 installiert ist.

10.5 IPSEC

Bestandteil der Windows-2000-Architektur ist auch eine Implementation des IPSEC-Standards, der eine sichere Übertragung von Daten auf IP-Ebene ermöglicht. Damit können im LAN oder im Internet Vertraulichkeit gewährleistet und virtuelle LAN (VLAN) in offenen Netzen betrieben werden. Durch die Verwendung eines offenen Standards sind diese Möglichkeiten nicht an den Einsatz von Windows 2000 gebunden.

Die IPSEC-Implementation von Windows 2000 verwendet die von Kerberos bereitgestellten Authentisierungsmechanismen. Im Rahmen von Sicherheits-Policies wird systemweit festgelegt, in welchem Umfang der von IPSEC zur Verfügung gestellte Schutz genutzt wird.

10.6 Wann ist der Wechsel auf Windows 2000 empfehlenswert?

Für den Wechsel von Windows NT auf Windows 2000 spricht aus Sicherheitserwägungen vor allem das Encryption File System. Bei der Verarbeitung schützenswerter Daten auf Laptops oder anderen räumlich gering geschützten Geräten oder bei der Speicherung besonders sensibler Daten ist dieser Schritt daher empfehlenswert.

Hinsichtlich der Umstellung in größeren Installationen ist zu beachten, dass einige der Vorteile von Windows 2000 nur dann zum Tragen kommen, wenn der Wechsel vollständig oder zumindest in wesentlichen Teilen erfolgt sowie andere, anwendungsspezifische Voraussetzungen gegeben sind.

Checkliste zur Prüfung von Windows NT

Die folgenden Fragen bilden eine Zusammenfassung der in den Kapiteln 5-9 beschriebenen Themen und dienen als Hilfestellung bei der Prüfung und Bewertung von NT-Systemen.

Bootschutz-Maßnahmen

- Wird das Laden eines anderen Betriebssystems durch entsprechende BIOS-Einträge verhindert?
- Können die BIOS-Einträge nur nach erfolgreicher Eingabe eines BIOS-Passworts geändert werden?
- Wird das unbefugte Öffnen des Gerätes durch ein Gehäuseschloss verhindert?

NT-Installation

- Ist NTFS als Dateisystem installiert?
- Wird das NT-Netz als Domäne betrieben?
- Sind Mail-Server in einer eigenen Domäne untergebracht?
- Existieren Vertrauensbeziehungen zwischen fremden Domänen, in denen sensible personenbezogene Daten verarbeitet werden?
- Stehen den Benutzern Disketten- oder CD-ROM-Laufwerke zur Verfügung?
- Steht elektronische Post internetweit bzw. intranetweit am Arbeitsplatz zur Verfügung?
- Steht Web-Zugriff internetweit bzw. intranetweit am Arbeitsplatz zur Verfügung?
- Kann der NT-Server nur von hierfür autorisierten Benutzern heruntergefahren werden?
- Wird der Zugriff auf Systemressourcen durch den Systemrichtlinien-Editor (policies) eingeschränkt?

- Werden im Client-Server-Netzwerk sensible personenbezogene Daten lokal gespeichert?

NT-Administration

- Beträgt die Mindestlänge der Passwörter 6 Zeichen?
- Beträgt die Gültigkeitsdauer der Passwörter maximal 90 Tage?
- Enthalten die Passwörter Sonderzeichen?
- Werden neue Passwörter mit den letzten 5 zurückliegenden Passwörtern verglichen?
- Haben Benutzer Leserechte auf die Kopie der SAM-Datei im Verzeichnis *winnt\repair*?
- Wird das Programm Syskey zur zusätzlichen Verschlüsselung der SAM-Datei eingesetzt?
- Ist die Administratorkennung umbenannt worden?
- Ist die Gast-Kennung deaktiviert worden?
- Sind die Posix- und OS/2-Subsysteme gelöscht worden?
- Ist der Zugriff auf die Registry-Editoren *regedt32* und *regedit* für Benutzer gesperrt?
- Können Kennungen mit privilegierten Systemverwalterrechten nur von bestimmten Arbeitsplätzen aus aufgerufen werden?
- Können Kennungen, mit denen auf sensible personenbezogene Daten zugegriffen werden kann, nur von bestimmten Arbeitsplätzen aus aufgerufen werden?
- Welche Ereignisse werden protokolliert?
 - fehlerhaftes An- und Abmelden
 - fehlerhafte Dateizugriffe
 - fehlerhafte Verwendung von Benutzerrechten
 - erfolgreiche und fehlerhafte Aktivitäten der Benutzer- und Gruppenverwaltung
 - erfolgreiche und fehlerhafte Änderungen der Sicherheitsrichtlinien
 - erfolgreiches und fehlerhaftes Neustarten und Herunterfahren des Servers
 - sämtliche Remote-Zugriffe
 - Zugriffe auf die Server-Registry
 - Zugriffe auf Unterverzeichnisse bzw. Dateien, in denen sensible Dokumente gespeichert sind
- Werden die Systemprotokolle unter einer eigens hierfür eingerichteten Revisorkennung ausgewertet?
- Welche Systemverwalterkennungen sind eingerichtet worden und werden auch benutzt?
 - Domain-Administratoren
 - Administratoren (Eigentümer von Inhaltsverzeichnissen und Dateien)
 - Sicherheits- und Replikations-Operatoren
 - Revisoren

- Ist den Domain-Administratoren der Zugriff auf sensible Daten entzogen worden?

Remote Access Service (RAS)

- Erfolgt ein Remote-Zugriff auf die Administratorkennung?
- Erfolgt der Verbindungsaufbau per CHAP-Verfahren?
- Wird die RAS-Verbindung verschlüsselt?
- Ist der Remote-Zugriff nur über bestimmte Endgeräten erlaubt?
- Erfolgt der Remote-Zugriff über den RAS-Server hinaus auch auf andere Rechner?
- Wird er Remote-Zugriff protokolliert?

Internetzugang

- Kann während der Nutzung von elektronischer Post auf sensible personenbezogene Daten zugegriffen werden?
- Erfolgt die Nutzung von elektronischer Post unter einer eigenen Benutzerkennung?
- Kann während der Internetnutzung auf sensible personenbezogene Daten zugegriffen werden?
- Erfolgt der Internetzugang unter einer eigenen Benutzerkennung?
- Werden TCP/IP-Ports für einzelne IP-Adressen durch Router oder Firewall gefiltert?
- Werden TCP/IP-Ports für einzelne Benutzer durch Router oder Firewall gefiltert?

System Management Service (SMS)

- Muss der Remote-Zugriff auf den Arbeitsplatz-PC explizit durch den Benutzer freigegeben werden?
- Wird der Remote-Zugriff auf den Arbeitsplatz-PC deutlich erkennbar angezeigt?
- Hat der Software-Installierer Zugriff auf den Installations-Ordner?
- Sind die Programme des Package-Control-Managers installiert?

Quellenhinweise zu Windows NT

Bücher

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch.

Kühn, U.; Schläger, U.: Datenschutz in vernetzten Computersystemen. Frechen 1997

Sheldon, T.: Windows NT Security Handbook. Osborne McGraw Hill, Berkeley 1997

Microsoft-Unterlagen

Encrypting File System for Windows 2000, Microsoft Corp., 1998

Windows 2000 Security—Default Access Control Settings, Microsoft Corp., 1999

Windows 2000 Kerberos Authentication, Microsoft Corp., 1999

Single Sign-On in Windows 2000 Networks, Microsoft Corp., 1998

Sicherheits-Leitfäden

Secure Windows NT Installation und Configuration Guide (US Navy)
(infosec.nosc.mil/TEXT/COMPUSEC/navynt.zip)

Windows NT Security Guidelines (Studie der Firma Trusted Systems Services im Auftrag der National Security Agency, USA) (www.TrustedSystems.com/fm_Signup.htm)

Interessante Webseiten

www.it.kth.se/~rom/ntsec.html

www.ntbugtraq.com

www.w3.org/Security/Faq/www-security-faq.html

www.somarsoft.com/security.htm

www.iss.net/vd/librarysitesn.html

www.iss.net/xforce

Mailing-Listen

NTBUGTRAQ von Russ Cooper, Anmeldung erfolgt per E-Mail bei listserv@listserv.ntbugtraq mit dem Befehl *subscribe ntbugtraq* <Vorname> <Nachname>

ISS-NT-Security von Internet Security Systems (www.iss.net/vd/maillist.html)

Tools zur Überprüfung der NT-Sicherheit

System Security Scanner:

Von der Firma ISS wird zum Test von NT-Systemen das Produkt System Security Scanner angeboten. Der System Security Scanner ermöglicht im Auftrag und unter Kontrolle des verantwortlichen Systemverwalters Brute-force-Attacken zum Erraten von Passwörtern, Denial-of-Service-Attacken, lokales Portscannen, das Aufdecken von NFS-, RPC-, Net-BIOS-Schwachstellen sowie eine Überprüfung sicherheitskritischer Registry-Parameter.

Kane Security Analyst:

Der Kane Security Analyst überprüft WindowsNT-Netze auf bekannte Sicherheitslücken. Neben Denial-of-Service-Attacken und Brute-Force-Attacken zum Erraten von Passwörtern werden Test zum Aufdecken von NFS- und Net-BIOS-Schwachstellen sowie eine Bewertung der Registry-Parameter durchgeführt.

Microsoft C2 Konfiguration Manager:

Das Windows NT Ressource KIT von Microsoft (Service Pack 3) enthält den C2-Konfiguration-Manager. Er dient als Abbild der C2-Sicherheitskriterien aus schließlich zur Überprüfung der C2-Mechanismen und ist vom Funktionsumfang nicht mit den anderen Sicherheitstools vergleichbar.