Studienarbeit

Sicherheitslücken von Microsoft Windows 2000 und Gegenmaßnahmen

von
Kai Dittberner und Marc Poli

August 2001

Universität Hamburg
Fachbereich Informatik
Arbeitsbereich AGN
Betreuer: Prof. Dr. K. Brunnstein

Erklärung:
Wir versichern, dass wir die vorliegende Arbeit selbstständig, ohne fremde Hilfe angefertigt haben und keine außer den angegebenen Quellen und Hilfsmitteln benutzt haben.

Hamburg, 21. August 2001

.

Inhaltsverzeichnis

Vorwort

Diese Studienarbeit befasst sich mit den Sicherheitsproblemen des Microsoft Windows 2000 Betriebssystems in den erhältlichen Varianten Professional und Server-Versionen und erläutert mögliche Gegenmaßnahmen.

Die Arbeit wurde als Gruppenarbeit am Arbeitsbereich *Anwendungen der Informatik in Geistes- und Naturwissenschaft* (AGN) am Fachbereich Informatik der Universität Hamburg angefertigt.

Aus den Erfahrungen und dem Umgang mit Microsoft Windows Betriebssystemen wuchs das Interesse an deren Sicherheit. Die Positionierung von Windows 2000 als professionelles Betriebssystem und die verstärkt auftretenden Sicherheitsprobleme in vernetzten Systemen bildeten die Grundlage für diese Studienarbeit.

Aufteilung

Die Aufteilung der Studienarbeit erfolgte anhand der Erfahrungen der Autoren und ist im folgenden aufgelistet:

Diese Kapitel der Studienarbeit wurden von beiden Autoren verfasst:

	Vorwort
Kapitel 1	Einleitung
Kapitel 2	Das Microsoft Windows 2000 Betriebssystem
Kapitel 2.1	Sicherheitsrelevante Komponenten von Windows 2000
Kapitel 2.2	Integrierte Komponenten von Windows 2000
Kapitel 3	Verschiedene Angriffstaktiken
Kapitel 4	Sicherheitsprobleme der Komponenten und Gegenmaßnahmen
Kapitel 4.1	Sicherheitsrelevante Komponenten
Kapitel 4.2	Integrierte Komponenten
Kapitel 5	Vermeidung von Sicherheitsproblemen
Kapitel 5.2	Administrative Einstellungen in Windows 2000
Kapitel 5.3	Überwachung
Kapitel 6	Zusammenfassung
Kapitel 7	Ausblick

Die weiteren Abschnitte in den Kapiteln 2 und 4 wurden wie folgt aufgeteilt:

Marc Poli	Windows Inside, Access Control, Encrypting File System, Netzwerk, Kerberos v5, Infrastruktur öffentlicher Schlüssel, IPSec und FileServer
Kai Dittberner	Active Directory, Component Object Model, Dynamic Host Configuration Protocol, NetBIOS-Namensdienst und WINS, Domain Name System, Internet Information Server 5.0, Active Server Pages und Terminaldienste.

Die Angrifftechniken in Kapitel 3 sind folgendermaßen aufgeteilt worden:

Marc Poli	Port-Scanning, Spoofing, Connection Hijacking, Denial-of-Service Angriffe, Replay Attacken, Rootkits, Backdoors, Tastaturaufzeichnung
Kai Dittberner	Passwortangriffe, Sniffing- und Man-in-the-Middle-Angriffe, Trojaner, Webangriffe, Pufferüberläufe

In Kapitel 5 wurde das Kapitel 5.1 von Marc Poli und Kapitel 5.4 von Kai Dittberner bearbeitet.

1 Einleitung

Ein immer größer werdendes Bedürfnis nach sicheren Systemen führt zu einer vermehrten Suche nach einem leicht zu sichernden und konfigurierbaren System. Diese Studienarbeit soll einen Einblick darüber geben, ob Windows 2000 diese Kriterien erfüllt und wie sicher das Gesamtkonzept des Betriebssystems in seinen Komponenten von Microsoft durchgesetzt wurde.

In Kapitel 2 werden die sicherheitsrelevanten und internen Komponenten von Windows 2000 analysiert und hiermit der Grundstein für die Sicherheitsanalyse in Kapitel 4 gelegt.

Kapitel 3 enthält eine Zusammenfassung sämtlicher aktiver Angriffsarten auf Computer, die in der Effektivität auf Windows 2000 Systeme bewertet werden.

In Kapitel 4 werden vorhandene Sicherheitslücken diskutiert und Gegenmaßnahmen oder Empfehlungen zur Verbesserung der Systemsicherheit angeboten.

Kapitel 5 enthält einen allgemeinen,sicherheitsrelevanten Teil, der auf alle Computersysteme zutrifft, und einen Abschnitt, der sich speziell mit der Konfiguration von Windows 2000 befasst.

2 Das Microsoft Windows 2000 Betriebssystem

Microsoft Windows 2000 ist das jüngste der professionellen Betriebssysteme von Microsoft und der direkte Nachfolger des im Sommer 1996 vorgestellten Microsoft Windows NT 4.0, auf dem Windows 2000 basiert und dessen Leistungsspektrum um einige neue Komponenten und eine überarbeitete Benutzerschnittstelle erweitert.
Die Entwicklungszeit betrug dreieinhalb Jahre und im Dezember 1999 wurden die verschiedenen Versionen, Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server und Windows 2000 Datacenter Server veröffentlicht. Seit dem wurden zwei Service Packs und einige wichtige Updates herausgegeben, die bereits bekannt gewordene Fehler beheben.

Die unterschiedlichen Windows 2000 Versionen

Microsoft Windows 2000 ist in unterschiedlichen Versionen für den Einsatz als Client- bzw. Einzelsystem oder als Serverversion erhältlich.

Edition	Anzahl der unterstützten Prozessoren	Unterstützte physische Speichergröße	Anzahl der unterstützten gleichzeitigen Client-Netzwerkverbindungen*	Zusätzliche geschichtete Dienste
Windows 2000 Professional	2	4 GB	10	
Windows 2000 Server	4	4 GB	Unbegrenzt	Kann fungieren als Domänencontroller, Active Directory-Dienst, RAID-Software, DHCP-Server (DHCP - Dynamic Host Configuration Protocol), DNS-Server (DNS - Domain Name System), DFS-Server (DFS - Distributed File System), Zertifikatsdienste, Remote-Installation und Terminaldienste
Windows 2000 Advanced Server	8	8 GB	Unbegrenzt	Zwei Knoten umfassende Cluster
Windows 2000 Datacenter Server	32	64 GB**	Unbegrenzt	Vier Knoten umfassende Cluster, Process Control Manager

* Die Lizenzvereinbarung für Windows 2000 Professional (die in der Datei \Winnt\System32\Eula.txt enthalten ist) besagt, dass der Lizenznehmer berechtigt ist, maximal zehn Computer oder andere elektronische Geräte an den Arbeitsplatzcomputer anzuschließen, um die Dienste des Produkte ausschließlich für Datei- und Druckerdienste, Internet-Informationsdienste und den Remotezugriff (einschließlich der gemeinsamen Nutzung von Verbindungen und Telefondiensten) zu nutzen. Diese Beschränkung wird hinsichtlich der gemeinsamen Nutzung von Dateien und Drucker sowie dem Remotezugriff überwacht, nicht jedoch in Bezug auf die Internet-Informationsdienste.

** Theoretische Größe, abhängig von der Verfügbarkeit kommerzieller Hardware wird u.U. eine geringere Speichergröße unterstützt.

Tabelle 2-1 „Unterschiede zwischen Windows 2000 Professional und den Server-Editionen" [SOL00]

Die verschiedenen Betriebssystemversionen unterscheiden sich durch unterschiedliche Unterstützung für Prozessoren, Arbeitsspeicher und Netzwerkverbindungen. Die Unterschiede sind in Tabelle 2-1 aufgeführt.
Im Unterschied zur Professional Version können die Serverversionen Serverdienste ausführen und z.B. als Domänencontroller eingesetzt werden. Dagegen sind die meisten internen Systemdateien, die Gerätetreiber, die wichtigsten Systemdienstprogramme und DLLs[1] identisch.
Die Professional Version wurde für den Einsatz als Arbeitsplatzsystem auf möglichst kurze Reaktionszeiten für den Benutzer optimiert, während die Serverversionen einen hohen Datendurchsatz gewährleisten sollen. Dafür werden bei einem Systemstart unterschiedliche Einstellungen am System vorgenommen, die es für die jeweilige Anwendung optimieret.

2.1 Sicherheitsrelevante Komponenten von Windows 2000

Windows 2000 wurde um eine Reihe von neuen Diensten und Komponenten erweitert, die die Sicherheit des Systems verbessern. Viele dieser Komponenten basieren auf bereits bekannten Internetstandards, wodurch die Verbreitung und Akzeptanz erhöht wird.
In diesem Zusammenhang werden die verschiedenen Standards, die in Windows 2000 Verwendung finden, analysiert. Die meisten dieser offenen Standards sind von der IETF[2] in den RFCs[3] festgehalten worden, die von der IETF Website (http://www.ietf.org) heruntergeladen werden können.
Allein das Vorhandensein der neuen sicherheitsrelevanten Komponenten reicht allerdings nicht aus, sie müssen auch eingesetzt und richtig konfiguriert werden. Dieses Kapitel gibt eine Übersicht über die neuen Sicherheitssysteme und welche Vorteile damit erzielt werden können.

2.1.1 Windows Inside

Für die Sicherheit eines Systems sind nicht nur offensichtliche Methoden wie Konten, Zugriffsbeschränkungen und Kennwörter wichtig, sondern auch weniger offensichtliche, die den Schutz des gesamten Systems garantieren. Dazu gehört die Einschränkung von Rechten für Benutzer und Anwendungen. Mit eingeschränkten Benutzerkonten sollte man beispielsweise den Rechner nicht neu starten oder Software installieren können. Anwendungen könnten die Anwendungen anderer Benutzer oder das Betriebssystem manipulieren und sollten deswegen in einem eingeschränkten Kontext ausgeführt werden.

Sicherheitseinstufung

Die Sicherheitseinstufung für TCSEC[4] vom NCSC[5], einer Abteilung der NSA[6], die dem „Orange Book" entsprecht, wird wahrscheinlich C2 sein, da Windows NT 3.51 mit Service Pack 3 und

1 Dynamic Link Library (DLL) - Eine DLL enthält Programmcode, der von anderen Programmen genutzt werden kann.
2 Internet Engineering Task Force (IETF)
3 Request for Comment (RFC), Dokument ,das Internet-Protokolle und -Methoden definiert.
4 Trusted Computer System Evaluation Criteria
5 National Computer Security Center

Windows NT 4.0 mit Service Pack 6a, C2 zertifiziert wurden und Windows 2000 eine Weiterentwicklung des Sicherheitsmodells von Windows NT 4.0 ist. „...C2 gilt als höchste Einstufung, die für kommerzielle Betriebssysteme ausreichend und praktikabel ist“ [SOL00].

Folgende Kriterien sind für eine C2-Einstufung erforderlich:

- Eine sichere Anmeldefunktion, die nur nach Authentifizierung des Benutzers Zugriff gewährt.
- Eine wahlfreie Zugriffssteuerungsfunktion; hier kann der Besitzer einer Ressource entscheiden, wer und wie derjenige diese Ressource nutzen kann.
- Eine Sicherheitsüberwachung, mit der alle sicherheitsrelevanten Ereignisse und Zugriffsversuche erkannt und aufgezeichnet werden können, so dass man nachvollziehen kann, wer versucht hat unerlaubt Zugriff zu erlangen.
- Ein Schutz vor Objektwiederverwendung, der verhindert, dass Benutzer auf Speicher, der von anderen Benutzern wieder freigegeben wurde, zugreifen und den Inhalt auslesen können. Dies wird durch sofortige Initialisierung freigegebenen Speichers vor erneuter Zuteilung realisiert.

Zusätzlich gibt es in Windows 2000 zwei Formen der Zugriffssteuerung auf Objekte:

1. Wahlfreie Zugriffsteuerung. Hierbei wird dem Benutzer bei der Anmeldung ein Sicherheitskontext zugeordnet und bei dem Zugriff auf Objekte wird überprüft, ob die Berechtigungen hierfür bestehen. Des Weiteren kann der Benutzer seine eigenen Objekte (z.B. Dateien, Drucker) anderen zur Verfügung stellen, indem er sie freigibt (Netzwerkfreigabe über Fileserver / SMB / CIFS).
2. Privilegierte Zugriffssteuerung. Diese kann notwendig werden, wenn die wahlfreie Zugriffssteuerung nicht ausreicht. Es wird sichergestellt, dass auf geschützte Objekte zugegriffen werden kann, wenn der Besitzer nicht erreichbar oder eventuell ein Angestellter ist, der das Unternehmen verlassen hat. In diesem Fall kann der Administrator auf die Objekte zugreifen und die Zugriffsrechte dieser Objekte ändern.

Folglich erfüllt Windows 2000 die C2-Kriterien höchstwahrscheinlich, dieses muss aber noch durch das NCSC überprüft werden, was bei Windows NT 4.0 bereits längere Zeit in Anspruch genommen hat.

Eine weitere Einstufungsmöglichkeit bieten die so genannten „Common Criteria“, eigentlich CCITSE[7], die sich als multinationaler Standard für Produktsicherheit durchsetzen. Diese Spezifikation ist flexibler als TCSEC und beinhaltet die Konzepte des Sicherheitsprofils (PP – Protection Profile) und des Sicherheitsziels (ST – Security Target). Wahrscheinlich wird Windows 2000 nach diesen Kriterien bewertet, da die US-Regierung nicht mehr nach TCSEC evaluiert.

---

6 National Security Agency

7 Common Criteria for Information Technology Security Evaluation

Windows-Kernel

Windows 2000 enthält einen *Micro-Kernel*. Das ist ein sehr kleiner Kernel, der nur einfache Funktionen, wie etwa hardware exception handling, beherrscht. Der hardwarespezifische Code steht im HAL *(Hardware Abstraction Layer)*, der Hardwareabstraktionsschicht. Sie ermöglicht einfache Portierungen auf neue Prozessorarchitekturen, wie z.B. den Intel Itanium IA-64, der ein 64-Bit Prozessor ist und die nächste Prozessorgeneration von Intel darstellt. Das Betriebssystem läuft im *protected mode*, auch *Kernelmodus* genannt, und hat damit direkten Zugriff auf den Hauptspeicher und die weitere Hardware. Die meisten Anwendungen werden im *Benutzermodus* ausgeführt und haben keinen direkten Hardwarezugriff. Sie müssen daher „*system-calls*" benutzen, das sind Systemaufrufe, die über das API *(Application Programming Interface)* auf die Hardware zugreifen.

Windows 2000 benutzt zwei Prozessorzugriffsmodi, Intel Prozessoren beherrschen vier: Ring 0 bis Ring 3. Der Kernelmodus verwendet die Berechtigungsstufe 3 (Ring 3) und der Benutzermodus Stufe 0 (Ring 0). Damit kann man verhindern, dass Benutzeranwendungen Betriebssystemdaten oder -komponenten manipulieren können. Zusätzlich kann hiermit auch größtenteils ausgeschlossen werden, dass das Fehlerverhalten von Anwendungen die Stabilität des Systems gefährdet. Generell verfügt jeder Win32-Prozess über einen eigenen privaten Speicherbereich. Im Kernelmodus ausgeführter Betriebssystem- und Gerätetreibercode teilt sich jedoch einen virtuellen Adressbereich, wobei es keinen Schutz für privaten im Kernelmodus ausgeführten Speicher gibt. Da fast der gesamte Windows 2000-Betriebssystemcode im Kernelmodus ausgeführt wird, ist es sehr wichtig, dass andere Software, die im Kernelmodus läuft, streng getestet und gut implementiert wurde, um die Systemsicherheit nicht zu gefährden. Dies gilt auch für Gerätetreiber von Fremdherstellern, da diese, sobald sie im Kernelmodus arbeiten, uneingeschränkten Zugriff auf Betriebssystemdaten haben. „Das bedeutet, dass jede Betriebssystemkomponente und jeder Gerätetreiber potenziell Daten beschädigen kann, die von anderen Betriebssystemkomponenten verwendet werden." [SOL00]. Aus dieser Problematik heraus wurde der Treibersignaturmechanismus eingeführt, der den Benutzer bei der Installation eines von Microsoft nicht autorisierten und somit nicht anerkannten Treibers eines Fremdherstellers warnt, die Installation auf Wunsch des Benutzers jedoch durchführt. Im Benutzermodus ist der Zugriff auf Systemdaten beschränkt, es kann nicht direkt auf Hardware zugegriffen werden und es sind nicht alle Schnittstellen verfügbar. Wenn eine Anwendung im Benutzermodus einen Systemdienst (z.B. Datei öffnen) aufruft, fängt der Prozessor dieses ab und schaltet den Prozess in den Kernelmodus. Bei Beenden des Systemdienstes wird der Prozess wieder in den Benutzermodus geschaltet und der Benutzer kann weiterarbeiten.

Der Schutz des Arbeitsspeichers wird durch vier Methoden erreicht:

- Von Kernelmoduskomponenten genutzter Speicher darf nicht von Benutzermodusprozessen zugegriffen werden, geschieht dies dennoch, wird eine Zugriffsverletzung an den Prozess zurückgegeben.
- Jeder Prozess besitzt einen eigenen privaten Adressraum, auf den andere Prozesse nicht zugreifen können. Eine Ausnahme bilden Speicherseiten, die von Prozessen gemeinsam genutzt werden. Beim Zugriff überträgt die Speicherverwaltung von Windows 2000 die virtuelle

in eine physische Adresse und überprüft die Zugriffsberechtigung. Somit ist sichergestellt, dass Prozesse nicht auf Speicherbereiche von anderen Prozessen zugreifen können.
- Alle von Windows 2000 unterstützten Prozessoren bieten in irgendeiner Form Speicherschutz in Hardwareform an. Beispielsweise können Seiten auf diese Weise als schreibgeschützt gekennzeichnet werden.
- Abschnitte gemeinsamen Arbeitsspeichers verfügen über Standard Windows 2000 *Zugriffssteuerungslisten* (ACLs – Access Control Lists), die bei Zugriff überprüft werden. Somit dürfen nur Prozesse mit Erlaubnis auf diese gemeinsamen Speicherbereiche zugreifen. Hierbei wird auch beim Erstellen eines Speicherabschnitts für eine Speicherzuordnungsdatei überprüft, ob der erstellende Prozess die Berechtigung zur Durchführung besitzt. Er darf dies nur, wenn er zumindest Lesezugriff auf das zu Grunde liegende Dateiobjekt hat. Außerdem überwacht die Speicherverwaltung auch die Änderung der Attribute von Speicherabschnitten durch Prozesse, deren Rechte in den ACLs stehen, die beispielsweise für Seitenschutzverfahren (z.B. Copy-On-Write) nötig sind und lässt diese nur bei Berechtigung zu.

Das Sicherheitssystem von Windows 2000 besteht aus folgenden Komponenten:

- Dem *Process Manager*, der Prozesse mit Hilfe von Kernelfunktionen startet und beendet.
- Dem *Virtual Memory Manager*, der den virtuellen Speicher realisiert, um jeder Anwendung einen privaten Adressbereich zuweisen zu können.
- Dem *I/O Manager*, der ein geräteunabhängiges I/O-System für Prozesse zur Verfügung stellt und I/O-Anfragen zu den richtigen Gerätetreibern auflöst.
- Der *Local Procedure Call (LPC) Facility*, die eine schnelle, vereinfachte Version von *Remote Procedure Call* (RPC - Remoteprozeduraufruf) für die Kommunikation der Komponenten innerhalb eines Computers bereitstellt.
- Dem *Sicherheitsreferenzmonitor* (SRM – Security Reference Monitor), der Berechtigungen für den Zugriff auf Objekte überprüft, Benutzerrechte überwacht und Sicherheitsüberwachungsnachrichten ausgibt.
- Dem *Teilsystem der lokalen Sicherheitsinstanz* (Lsass – Local Security Authority Subsystem), das die Anwendung ‚lsass.exe' ausführt. Sie ist für die lokalen Sicherheitsrichtlinien, die bestimmen, wer sich an dem Rechner anmelden darf, die Berechtigungen der Benutzer, die Kennwort- und Überwachungsrichtlinien, die Benutzerauthentifizierung und das Senden von Sicherheitsüberprüfungsnachrichten zuständig. Für die Durchführung wird die Bibliothek ‚lsasrv.dll' von Lsass geladen, die den lokalen *Sicherheitsauthentifizierungsdienst* darstellt.
- Der *Lsass-Richtliniendatenbank*, die die lokalen Sicherheitsrichtlinien in der Registrierung im Schlüssel HKEY_LOCAL_MACHINE\SECURITY speichert.
- Der *Sicherheitskontenverwaltung* (SAM – Security Accounts Manager), die aus einer Reihe von Subroutinen besteht und als die Bibliothek ‚samsrv.dll' im Lsass-Prozess ausgeführt wird. Sie ist für die Datenbank verantwortlich, in der auf dem lokalen System die Benutzer- und Gruppeninformationen gespeichert werden.
- Der *SAM-Datenbank*, die die im lokalen System angelegten Benutzer und Gruppen, sowie deren Kennwörter und weitere Daten enthält. Sie wird in der Registrierung unter dem Schlüssel HKEY_LOCAL_MACHINE\SAM gespeichert.

- Dem *Active Directory*, einem Verzeichnisdienst, der in der Bibliothek ‚ntdsa.dll' implementiert ist und im Lsass-Prozess ausgeführt wird.
- Den *Authentifizierungspaketen*, die aus DLLs bestehen, die bei der Anmeldung eines Benutzers ausgeführt werden und die Authentifizierungsrichtlinien von Windows 2000 durchsetzen. Sie überprüfen Namen und Passwörter und geben bei richtiger Eingabe Informationen zum Sicherheitsprofil des Benutzers an Lsass zurück.
- Dem *Anmeldeprozeß* (WinLogon), der in der Datei ‚winlogon.exe' implementiert ist und auf die Anmeldetastenkombination *(SAS – ‚Strg+Alt+Entf')* wartet, um das Eingabefenster anzuzeigen und nach erfolgter Anmeldung die Bedienoberfläche zu laden.
- Der *Grafischen Identifikation und Authentifizierung* (GINA – Graphical Identification and Authentication), die aus der Bibliothek ‚msgina.dll' besteht, von WinLogon ausgeführt wird und auf die Eingabe von Name und Kennwort oder die PIN für eine Smartcard wartet.
- Dem *Netzwerkanmeldedienst* (Netlogon), der aus der Bibliothek ‚netlogon.dll' besteht und zur Netzwerkanmeldung von Microsoft LAN Manager 2 Windows NT, der Vorversion von Windows 2000, verwendet wird. Er beinhaltet einen Suchdienst für Domänencontroller.
- Dem *Window Manager and Graphical Device Interface* (GDI), dem Kernelmodusteil des Win32-Subsystems, der Benutzer-Eingaben und Bildschirm-Ausgaben abhandelt. Bei Windows NT wird Win32 im Benutzermodus ausgeführt, er wurde aber aus Performancegründen teilweise bei Windows 2000 in den Kernelmodus umgelegt.
- Dem *Kernelsicherheitsgerätetreiber* (KsecDD – Kernel Security Device Driver), der *Kernelmodusbibliothek* Ksecdd.sys, die die LPC-Schnittstellen implementiert und die Sicherheitskomponenten (z.B. das EFS – Encrypting File System) verwenden, um mit Lsass im Benutzermodus zu kommunizieren.
- Dem *Objekt-Manager*, der für die Sicherheit eine entscheidende Komponente ist, da er Objekte im Kernelmodus auf Anfrage an Benutzermodusprozesse exportiert und dafür die Berechtigungen des Benutzers überprüft. Bei der Anforderung von Objekten ist daher immer der Objekt-Manager in Verbindung mit dem Sicherheitssystem für die Auslieferung oder Zurückhaltung des Objekts verantwortlich.

  Das Sicherheitsmodell von Windows 2000 ist so angelegt, dass ein Prozess beim Zugriff auf ein Objekt von vornherein angeben muss, welche Operation mit dem Objekt durchgeführt werden soll. Die Berechtigung für die angegebene Operation wird dann geprüft und, wenn erfolgreich, ein Handle für den Prozess ausgegeben, in dem die Zugriffsberechtigungen stehen.
- Dem *Identitätswechsel* (Impersonation), der ein wichtiges Feature von Windows 2000 ist und oft zum Einsatz kommt. Beispielsweise wäre es zu aufwendig, wenn ein Benutzer aus der Ferne auf einem Server eine Datei löschen will, sämtliche Berechtigungen, die für diese Operation notwendig sind, an jeder Stelle zu überprüfen. Deshalb wurde der Identitätswechsel eingeführt, mit dem der Server, auf dem die Datei gelöscht werden soll, kurzfristig die Identität des Benutzers für die Ausführung dieses Prozesses annimmt und somit auch gleich seine Rechte besitzt, was aufwendige Zugriffsprüfungen überflüssig macht. Nach Ausführung der Operation kehrt der Server in sein normales Sicherheitsprofil zurück. Dies geht jedoch nur, wenn man sich auf dem Server anonym anmelden kann (Nullsitzung) und keine Anwendung ausführen möchte. Zur Anwendungsausführung muss sich ein Benutzer mit *LogonUser* und einer Parameterübergabe an dem Server anmelden. Dann ist es so, als würde sich der Benutzer interaktiv am Server anmelden und die Anwendung dort starten. Eine zweite Möglichkeit

hierfür bietet der Befehl *CreateProcessAsUser*, mit dem ein Server, wenn er eine Kopie des Benutzertokens besitzt, für diesen eine Anwendung starten kann. Bei den beiden letzten Möglichkeiten besteht jedoch das Problem, dass Kontoname und Kennwort verifiziert werden müssen und dies evtl. über ein Netzwerk geschieht, wobei diese Kommunikation sicher verschlüsselt werden müsste, damit die Zugangsdaten nicht abgefangen werden können. Zur Steigerung der Sicherheit darf ein Server nur die Identität des Benutzers annehmen, wenn dieser es erlaubt hat. Der Benutzer kann zusätzlich definieren, welche Ebene eines Identitätswechsels der Server für ihn durchführen darf, und zwar mit Hilfe des SQoS-Flags *(Security Quality of Service)*. Dafür gibt es vier Ebenen: 1.Security Anonymous: der Server darf weder Identität des Benutzers abfragen noch annehmen; 2.Security Identification: der Server darf Identität und Berechtigungen abfragen, jedoch nicht die Identität annehmen; 3.Security Impersonation: der Server kann Identität überprüfen und diese auf einem lokalen System annehmen; 4.Security Delegation: der Server kann sich auf lokalen und Remotesystemen für den Benutzer ausgeben. Letztgenannte Variante ist sehr freizügig und war unter Windows NT 4.0 nur eingeschränkt möglich. Ohne Vorgabe durch den Benutzer ist Security Impersonation voreingestellt.

Der *Benutzermodus* wird über die *‚ntdll.dll'* bereitgestellt, als Umgebungssubsystem bezeichnet *(environmental subsystem)* und besteht aus der folgenden Komponente: dem *Win32 Subsystem*, das im Benutzermodus ausgeführt wird, ein vom Betriebssystem benötigter Part ist und beim Bootvorgang des Systems geladen wird. Er besteht aus den Win32 API-DLLs *(kernel32.dll, user32.dll, gdi32.dll)* und dem Win32-Subsystem Prozess *(csrss.exe)*. Optional können noch Komponenten zur möglichen Ausführung von POSIX und OS/2 Anwendungen installiert und gestartet werden.

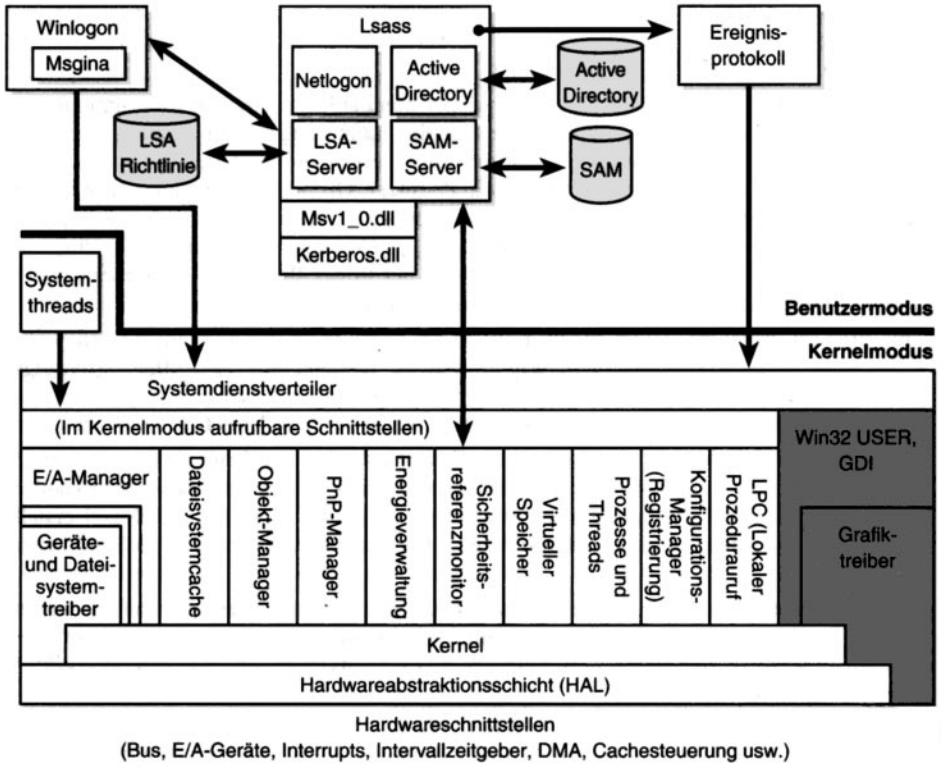

Abbildung 2-1 „Sicherheitskomponenten von Windows 2000" [SOL00]

Beim Systemstart stellen Lsass und der Sicherheitsreferenzmonitor über LPC eine Verbindung her und kein Benutzermodusprozess kann mehr mit diesen eine Verbindung eingehen, da sie nach diesem Verbindungsaufbau keine Anforderungen mehr beantworten. Der erste Prozess, der gestartet wird, ist WinLogon. Dieser vergewissert sich, dass er die Kontrolle über die Arbeitsstation hat, indem er eine Sicherheitsbeschreibung generiert und somit nur Prozesse auf den Rechner Zugriff erhalten, wenn WinLogon dies genehmigt. Dann wird auf eine Benutzerinteraktion für die Anmeldung gewartet. Immer wenn ‚Strg+Alt+Entf' gedrückt wird, werden alle offenen Fenster ausgeblendet und es wird auf eine Eingabe gewartet. Damit ist sichergestellt, dass WinLogon den Desktop zur Anmeldung kontrolliert. Auf diese Weise sollen Trojanische Pferde an der Übernahme der Eingabefenster und dem Ausspionieren von Zugangsdaten gehindert werden.

Der Sicherheitsreferenzmonitor, der für die Sicherheit bei Betriebssystemen immer eine entscheidende Rolle spielt, setzt Sicherheitsrichtlinien auf dem lokalen Computer durch, schützt und überwacht Objekte zur Laufzeit und somit die Betriebssystemressourcen.

Discretionary Access Control (DAC), *security auditing* (Sicherheitsüberwachung) und *memory protection* (Speicherschutz) setzen Windows 2000 auf einen Level mit UNIX Systemen [NOR01].

2.1.2 Access Control

In diesem Abschnitt wird auf das Sicherheitsmodell von Windows 2000 eingegangen. Im Kern besteht es aus den *Sicherheitsbeschreibungen* (Security Descriptors – SDs) und den *Zugriffskontrolllisten* (Access Control Lists – ACLs). Alle Objekte, die einer Sicherung bedürfen (Dateien, Geräte, Prozesse, etc.), haben zugewiesene Sicherheitsbeschreibungen. Diese Objekte enthalten folgende Informationen:

- Den *Security Identifier (SID)* des Besitzers
- Den Security Identifier (SID) der primären Benutzergruppe
- Die *diskrete Zugriffskontrollliste* (Discretionary Access Control List – DACL)

Die Sicherheitsbeschreibungen

In einer *Objektsicherheitsbeschreibung* sind Informationen enthalten, die dem System sagen, wer auf ein Objekt wie zugreifen darf. Bei der Erstellung eines Objektes in einem Sicherheitskontext wird seine Sicherheitsbeschreibung mit Informationen gefüllt. Dafür gibt es drei Möglichkeiten. Erstens kann der erstellende Prozess die Sicherheitsbeschreibungen direkt zuweisen. Ist dies nicht der Fall, überprüft das System das übergeordnete Objekt nach vererbbaren Informationen für die Zugriffssteuerung. Trifft dies auch nicht zu, wird der Standardwert, der durch den jeweiligen Ressourcenmanager vorgegeben wird, übernommen.

Der Security Identifier (SID)

Windows 2000 stellt Benutzer, Gruppen, Rechner und Domänen durch Nummern dar, die Sicherheitskennungen genannt werden. Sie sind numerische Strukturen variabler Länge und haben folgende Struktur:

1. 8-Bit-SID-Revisionsstufe
2. 8-Bit-Zählung der enthaltenen Subautoritäten
3. 48-Bit, die bis zu drei SIDs für Kennungsautoritäten enthalten
4. Eine variable Anzahl von Subautoritäten-SIDs und relativen Kennungen *(Relative Identifiers – RID)*

Bei der Installation von Windows 2000 wird ein weltweit eindeutiger SID aus dem Installationsdatum und der MAC-Adresse (Hardware-Adresse) der Ethernetkarte, falls eine solche vorhanden ist, generiert, die den Rechner identifizierbar macht. Daran angefügt wird der RID, der für den ersten angelegten Benutzer 1000 ist. Der nächste Benutzer trägt den SID, gefolgt von der RID 1001. Somit ergibt sich auch für jeden Benutzer eine weltweit eindeutige Kennung. Es existieren eine Reihe von vordefinierten SIDs und RIDs im System, der Benutzer „Administrator" hat beispielsweise den RID 500 und der Benutzer „Gast" den RID 501. Die RIDs ab 1000 sind für die vom Administrator angelegten Benutzer vorgesehen und frei. Ein SID für den Administrator eines Rechners könnte so aussehen:

S-1-5-21-13124455-12541255-61235125-500.

Zugriffskontrolllisten (Access Control Lists – ACLs)

Einem Objekt werden durch ACLs Berechtigungen und Überwachungsanweisungen für den Kernel zugeordnet. Die Bestandteile einer ACL sind der Header, gefolgt von keinem, einem oder mehreren *Access Control Entrys* (ACEs). Eine ACL ohne ACEs nennt man Null-ACL. In Windows 2000 gibt es zwei Formen von ACLs, benutzerbestimmbare (discretionary) Zugriffskontrolllisten (DACLs), welche Zugriffsberechtigungen auf Objekte beschreiben, und System-Zugriffskontrolllisten (SACLs), die Überwachungsanweisungen für das System enthalten. Der ACL-Typ ergibt sich aus den Einträgen in den Listen. Es sind sechs Eintragstypen definiert:

- Zugriff auf die DACL verweigert.
- Zugriff auf die DACL gewährt.
- Zugriff verweigert, objektspezifisch. Verweigert den Zugriff auf eine oder mehrere Eigenschaften und schränkt die Vererbung in einer DACL ein.
- Zugriff gewährt, objektspezifisch. Gewährt den Zugriff auf eine oder mehrere Eigenschaften und schränkt die Vererbung in einer DACL ein.
- Systemüberwachung. Protokolliert Zugriffe auf die SACL.
- Systemüberwachung, objektspezifisch. Protokolliert Zugriffe auf eine oder mehrere Eigenschaften und schränkt die Vererbung in einer SACL ein.

Hierbei wird im ersten Fall über eine Identifizierung mittels der SID der Zugriff abgelehnt, im zweiten Fall wird er gewährt. Durch Systemüberwachung wird nach erfolgreicher Identifizierung der Zugriff gewährt und eine Protokolldatei geschrieben.

Eine Bitmaske mit Zugriffsrechten legt in der ACL fest, welche Vorgänge von Gruppen oder Benutzern an Objekten durchgeführt werden dürfen. Sie setzt sich aus vier Zugriffsarten zusammen:

- allgemeine: read, write, execute, all
- standardmäßige: delete, read control, synchronize, write_dac, write_owner
- SACL: Lesen und Ändern der Einstellungen für die Objektüberwachung
- objektspezifische: z.B. benötigen Drucker spezielle Rechte und andere nicht, hierunter fallen auch erweiterte Rechte, die durch globale eindeutige Bezeichner (Globally Unique Identifiers – GUIDs) gekennzeichnet sind

Für den Fall, dass die Sicherheitsbeschreibung eines Objekts keine DACL enthält, hat jeder Zugriff auf das Objekt. Falls eine DACL eines Objekts Null ist (keine ACE-Einträge enthält), kann nur der Besitzer auf das Objekt zugreifen. Dieser kleine Unterschied ist sehr entscheidend für die Sicherheit. Im Falle einer leeren SACL findet keine Überwachung statt.

Token

Bei der Anmeldung an einem Windows 2000-System erzeugt das System ein *Zugriffstoken* für den jeweiligen Benutzer. In diesem Token stehen sein SID, die SIDs aller Gruppen, denen er angehört, und seine Berechtigungen. Das Token markiert damit den Sicherheitskontext des Benutzers. Beim Start einer Anwendung erhält diese eine Kopie des Zugriffstokens, damit sie beim Aufruf eines geschützten Objekts die Berechtigung des Benutzers vorweisen und die Aktion durchführen kann.

Vererbung von Berechtigungen

Durch die *Vererbung von Berechtigungen* kann man einem Container, beispielsweise einem Ordner, Berechtigungen für den Zugriff zuweisen und diese auf alle enthaltenen Objekte vererben. Diese Rechte werden auch neuen Ordnern bei deren Erstellung in solch einem Container zugewiesen. Es ist möglich, die Berechtigungen für Ordner und alle enthaltenen Ordner mit einem Schritt zu ändern, somit kann man den administrativen Aufwand wesentlich verringern, da man nicht mehr die Berechtigungen jedes enthaltenen Objektes einzeln ändern muss.

2.1.3 Active Directory und Windows 2000 Domänen

Windows 2000 führt mit dem *Active Directory (AD)* einen Verzeichnisdienst ein, der viele fundamentale Funktionen im System übernimmt und erforderlich ist, sobald ein Windows 2000 Server zu einem *Domänencontroller (DC)* heraufgestuft wird. Dabei ist das AD im Grunde ein objektorientierter, hierarchisch aufgebauter Datenspeicher für strukturierte Informationen.

Offenes Design

Microsoft hat sich bei der Entwicklung des AD an eine Reihe von Internetstandards gehalten, die dazu beitragen sollen, es in viele Bereiche zu integrieren. So basiert der AD Verzeichnisdienst auf

dem *X.500 Verzeichnisschema* und kann über das *LDAP (Lightweight Directory Access Protocol)* Protokoll angesprochen werden.

X.500

Der X.500 Standard beschreibt mit seinen Regeln einen verteilten Verzeichnisdienst, der Informationen über die Benutzer und Ressourcen in einer Systeminfrastruktur enthält und über alle Server abrufbar ist. Das Active Directory ist nun von diesem X.500 Modell abgeleitet, es unterstützt allerdings nicht alle Kabelprotokolle, die in X.500 definiert sind. Nicht unterstützt werden *DAP[8], DSP[9], DISP[10] und DOP[11]*. Unterstützt und verwendet werden dagegen das genannte LDAP und aus Gründen der Kompatibilität *MAPI / RPC[12]*.

LDAP (Lightweight Directory Access Protocol)

Das AD ist vollständig zu LDAP [RFC1777] kompatibel. Verwendung finden die LDAP Protokolle LDAPv2 und LDAPv3 [RFC2251]. LDAP ermöglicht das Suchen und Modifizieren von Objekten im AD und kann z.B. über folgende APIs angesprochen werden:

- **LDAP C API**
  Eine Sammlung von in C geschriebenen APIs, die eine Portierung des Protokolls auf andere Systeme erleichtern sollen. Informationen über diese API sind im [RFC1823] zu finden.
- **ADSI API (Active Directory Service Interface)**
  ADSI ist eine von Microsoft entwickelte API, um Zugriff auf das AD zu erhalten. Es ist für die Novell NetWare Verzeichnisdienste, NetWare 3 und Windows NT verfügbar. ADSI unterstützt die Programmiersprachen C/C++, Visual Basic und VB für Applikationen.

Komponenten des AD (Objekte, Domänen, Standorte)

Das Active Directory ist ein Verzeichnisdienst, der die Aufgabe hat, Objekte und zugehörige Attribute in einer baumartigen Struktur zu speichern und zu verwalten. Der Verzeichnisdienst kann sich dabei über mehrere Server, Netzwerke und Standorte hinweg erstrecken, das Active Directory sorgt dafür, dass die Objekte und die Datenbank auf allen Systemen regelmäßig synchronisiert werden.
Unter Windows NT wurde die Verwaltung der Benutzer- und Sicherheitsinformationen von *primären Domänencontrollern (PDC)* und *Backup Domänen Controller (BDC)* übernommen und eine Änderung auf einem PDC wurde auf alle BDCs übertragen. Unter Windows 2000 gibt es nur noch Domänencontroller (DC) und alle DCs erlauben Änderungen an den Benutzer- und Sicherheitseinstellungen. Diese Informationen werden im Active Directory gespeichert und dann auf alle zugehörigen DCs repliziert. Diese Technik wird als *Multimaster-Replikation* bezeichnet.
Das AD ist allerdings ein allgemeiner Verzeichnisdienst, der neben Informationen über Netzwerkressourcen, Benutzer und Gruppen viele weitere Informationen enthalten kann. Durch die offene

8 Directory Access Protocol (DAP)

9 Directory System Protocol (DSP)

10 Directory Information Shadowing Protocol (DISP)

11 Directory Operational Binding Managment Protocol (DOP)

12 Remote Procedure Call (RPC), Methode, um Funktionen über ein Netzwerk aufzurufen.

Schnittstelle können auch andere Software-Hersteller auf das Active Directory zugreifen und eigene Informationen in ihm speichern.
Eine auf Active Directory basierende Domäne kann als reine Windows 2000 Domäne oder als Domäne mit Unterstützung für ältere NT 4.0 Backup-Domänencontroller eingerichtet werden, wodurch einige neue Funktionen deaktiviert werden, solange dieser *gemischte Modus* aktiv ist. Eine Umstellung auf eine reine Windows 2000 Domäne ist jederzeit möglich, einen Weg zurück in den gemischten Betrieb gibt es aber nicht.

Objekte und Container

Das Active Directory verwaltet Informationen verschiedener Art. Diese werden als Objekte in der AD Struktur gespeichert. Ein Objekt ist also ein Drucker, ein Benutzer, etc., das weitere Attribute besitzt, die vom Objekttyp abhängig sind. So wird ein Benutzer andere Attribute besitzen, als ein Drucker, der z.B. einen Standort hat, aber kein Passwort. Diese Objekttypen werden als Objektklassen bezeichnet, die die Art der Attribute bestimmen, die ein Objekt aufnehmen kann. Attribute können hinzugefügt und in einigen Fällen auch entfernt werden.
Sollen mehrere Objekte zusammengefasst werden, bietet das AD Container, die Objekte und weitere Container aufnehmen können.

Domänenstrukturen

Das Active Directory definiert eine Domänenstruktur, um Benutzer und Gruppen zu verwalten. Im Unterschied zum älteren Windows NT besteht allerdings keine besondere Notwendigkeit mehrere einzelne Domänen anzulegen, da das AD leistungsfähig genug ist, alle Informationen in einer *Domänenstruktur* zu verwalten. Durch die Verwendung von einem hierarchisch aufgebauten Namensraum für Domänen, ist es aber sinnvoll mehrere Domänen und Subdomänen einzusetzen, um bspw. die Struktur eines Unternehmens abzubilden. AD benutzt für die Verwaltung der Domänen das *Domain Name System (DNS)*, daher wird auch der *DNS-Namensraum* für die Domänennamen eingesetzt.
Domänen sind im AD also administrative Werkzeuge, so können administrative Rechte an andere Benutzer delegiert werden, diese haben dann die Aufgabe ihre *Organisationseinheiten (OUs)* zu administrieren. Es werden alle Einstellungen, Objekte und Richtlinien auf die Domänencontroller für diese Domäne repliziert.
Die Verwendung des Domain Name Systems macht sich auch in der Domänenstruktur bemerkbar. Domänen können Subdomänen enthalten, die zu einem Domänenbaum anwachsen und die Domänenstruktur darstellen.

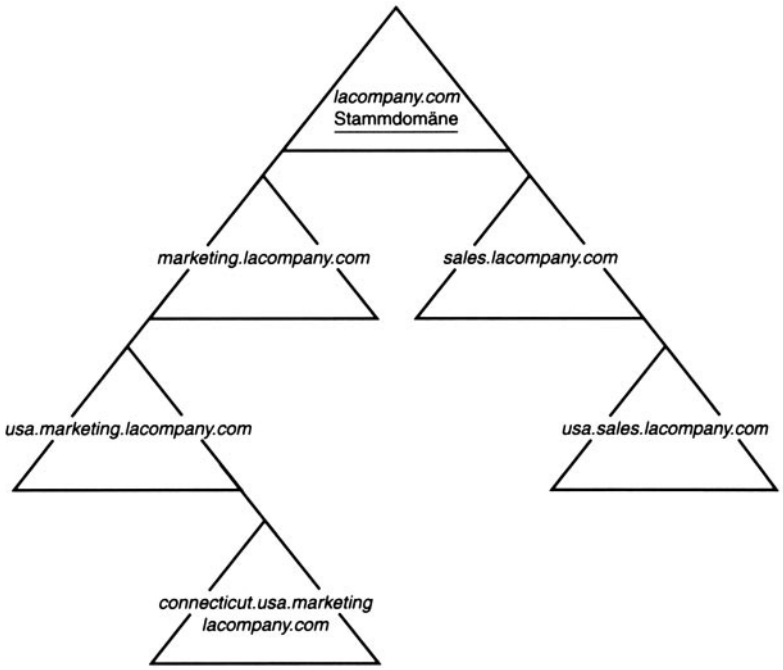

Abbildung 2-2 „Hierarchische Struktur eines Domänenbaums“ [SCH01]

Vertrauenseinstellungen werden für eine Domänenstruktur automatisch erstellt und sind transitiv. Vertraut Domäne 1 Domäne 2 und vertraut Domäne 2 Domäne 3, so vertraut auch Domäne 1 Domäne 3. Für die Überschreitung der Domänen wird das Kerberos Protokoll verwendet, dass die Domänen über die transitiven Vertrauenseinstellungen von Kerberos verbindet.

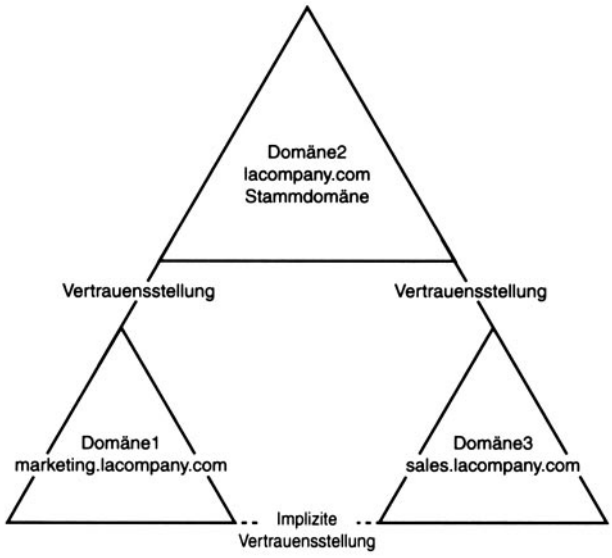

Abbildung 2-3 „Transitive Vertrauenseinstellungen“ [SCH01]

Domänengesamtstrukturen

Domänen werden in Domänenstrukturen zusammengefasst und mehrere Domänenstrukturen bilden eine Domänengesamtstruktur. Zwischen den Domänenstrukturen werden allerdings keine

automatischen Vertrauenseinstellungen erstellt. Die Einrichtung mehrere Domänenstrukturen ist sinnvoll, wenn die administrativen Aufgaben für unterschiedliche Domänen vollständig getrennt werden sollen.

Standorte

Windows 2000 bietet das erste Mal die Möglichkeit der Verwaltung von Standorten. Ein Standort ist dabei eine logische Menge von Domänencontrollern und Computern und dient hauptsächlich der Erhöhung der Effektivität der Replikation zwischen den DCs. Durch die Angabe der Verbindungsgeschwindigkeit zwischen zwei Standorten wird der Replikationsprozess automatisch optimiert. Replikationen innerhalb eines Standorts werden häufiger durchgeführt als zwischen Standorten, die meist über WAN[13]-Verbindungen verbunden sind. Außerdem können Zeitpläne für die Replikation zwischen Standorten erstellt werden, so dass diese z.B. nachts durchgeführt werden können.

Organisationseinheiten (OUs)

Die OUs sind Verzeichnisobjekte im AD, die Computer, Benutzer, Gruppen, Drucker, freigegebne Ordner und andere OUs aufnehmen können und im Verzeichnisdienst als Ordner dargestellt werden. Durch sie können die oben genannten Objekte zu logischen Einheiten kombiniert werden. Administrative Aufgaben innerhalb dieser Einheit können an Benutzer der Domäne, in der sich die Einheit befindet, delegiert werden. Dadurch kann die Verwaltung des Netzwerks verteilt werden, ohne dass jeder Administrator vollständige administrative Rechte über die Domäne erhalten muss.

Schema

Die AD-Objekte basieren auf Objektklassen, die angeben, welche Attribute ein Objekt dieser Klasse besitzt und welche Objekte als übergeordnete Objekte eingesetzt werden können. Diese Beschreibungen sind im AD-Schema festgelegt, wobei das Schema selbst im AD gespeichert wird und auch verändert werden kann. Allerdings sind nur wenige Änderungen möglich und diese auch mit Vorsicht vorzunehmen, da das Schema von einer Domänengesamtstruktur verwendet wird und jede Änderung auf alle Domänencontroller der Gesamtstruktur repliziert wird.
Es gibt zwei Objektgruppen im AD-Schema: Klassen und Attribute. Jedes Attribut wird im AD eindeutig definiert und kann dann in Objektklassen eingesetzt werden. Attribute können außerdem indiziert werden, so dass eine Suche deutlich schneller erfolgen kann. Auch die Indizierung eines Attributes erfolgt über die Objektklassen hinweg. Die Klassen definieren, ob ein Objekt ein Containerobjekt oder ein Endknotenobjekt ist. Containerobjekte können weitere Objekte enthalten (wie z.B. Ordner), Endknotenobjekte nicht. Die Klassen definieren, welche Attribute die Objekte enthalten können bzw. müssen.

Globaler Katalog (GC)

Der *Globale Katalog* ist eine Datenbank, die für Anmelde- und Suchabfragen an das AD verwendet wird. Das AD erzeugt mindestens einen GC automatisch, weitere GCs können hinzugefügt werden. Steigt die Zahl der GC-Server, wird die Antwortzeit einer Anmeldung oder Suchabfrage verbessert, allerdings steigt auch der Datenverkehr, der für die Replikation benötigt wird.

---

13 Wide Area Network (WAN), ein ausgedehntes Netzwerk, wie bspw. das Internet.

Betriebsmaster

Einige Änderungen am Active Directory können nur an einem bestimmten Domänencontroller vorgenommen werden, der als *Betriebsmaster* für die bestimmte Aufgabe bezeichnet wird. Die Aufgaben verbleiben auf dem zuerst installierten Domänencontroller, können aber später auf andere verteilt werden.
Folgende zwei Aufgaben, die die gesamte Domänenstruktur betreffen, müssen eindeutig zugewiesen werden:

- **Schemamaster**
  Der Domänencontroller, der die Aufgabe des *Schemamasters* übernimmt, ist der einzige Domänencontroller an dem Änderungen am Schema möglich sind.
- **Domänennamenmaster**
  Dieser Domänencontroller kontrolliert das Hinzufügen und Entfernen von Domänen in einer Domänenstruktur.

Die folgenden drei Aufgaben benötigen für jede Domäne einen Betriebsmaster

- **RID-Master**
  Jedes Mal, wenn ein Domänencontroller einen neuen Benutzer, eine neue Gruppe oder einen neuen Computer erstellt, bekommt dieses Objekt eine eindeutige *Sicherkeitskennung (SID)*. Die SID besteht aus einer domänenbezogenen Sicherheitskennung und einer *relativen Kennung (RID)*. Hat ein Domänencontroller seinen Vorrat an RIDs verbraucht, bekommt er vom *RID-Master* neue RIDs zugeteilt.
- **PDC-Emulator**
  Der *PDC-Emulater* dient als primärer Domänencontroller in gemischten Windows Systemumgebungen. Sind noch ältere NT 4.0 Backup Domänencontroller im Netz vorhanden, repliziert der PDC-Emulator Aktualisierungen an diese. Der PDC-Emulator hat außerdem eine höhere Priorität bei der Replikation von Kennwortänderungen. Schlägt eine Netzwerkanmeldung an einem anderen Domänencontroller fehl, leitet dieser die Anforderung an den PDC-Emulator weiter, bevor er die Anmeldung ablehnt.
- **Infrastrukturmaster**
  Der *Infrastrukturmaster* aktualisiert die Beziehungen zwischen den Objekten im AD. Wird bspw. ein Benutzer in eine andere Gruppe verschoben, sorgt der Infrastrukturmaster dafür, dass die Benutzer- und Gruppeninformationen auf allen Domänencontrollern aktualisiert werden. Ein Domänencontroller kann nur gleichzeitig Infrastrukturmaster sein und den Globalen Katalog besitzen, wenn er der einzige Domänencontroller ist. Befindet sich auf allen Domänencontrollern ein globaler Katalog, dann wird der Infrastrukturmaster nicht benötigt.

Multimaster-Replikation

Das Active Directory wird über alle Domänencontroller synchronisiert. Änderungen an einem Objekt im Active Directory eines Domänencontrollers werden an die anderen repliziert. Dieser Vorgang wird als *Multimaster-Replikation* bezeichnet. Dafür sind die im AD gespeicherten Informationen in drei Kategorien aufgeteilt. Domänencontroller, die einen Globalen Katalog (GC) enthalten, verwenden noch eine vierte Kategorie.

- **Verzeichnispartition für Domänendaten**
  Diese Kategorie enthält alle Objekte im Verzeichnis für die jeweilige Domäne. Die Objekte werden an alle anderen Domänencontroller dieser Domäne repliziert.
- **Verzeichnispartition für Schemadaten**
  Das Schema enthält die Informationen über die Objekte und die möglichen Attribute. Diese Daten werden an alle Domänencontroller in der Domänen- bzw. Domänengesamtstruktur repliziert.
- **Verzeichnispartition für Konfigurationsdaten**
  Diese Partition enthält Daten über die *Replikationstopologie* und Daten von Anwendungen, die das Active Directory verwenden. Auch diese Informationen werden an alle Domänencontroller in der Gesamtstruktur repliziert.
- **Partielles Replikat des Domänendaten-Verzeichnisses für alle Domänen**
  Diese Kategorie wird nur auf einem Domänencontroller verwendet, der einen Globalen Katalog enthält. Während ein Domänencontroller eine vollständige Kopie der Verzeichnisdaten seiner eigene Domänen enthält, die sowohl gelesen als auch geschrieben werden kann, enthält ein Domänencontroller mit einem globalen Katalog auch eine partielle Kopie der Verzeichnisdaten der anderen Domänen in der Gesamtstruktur, damit schneller auf diese zugegriffen werden kann. Diese Daten können allerdings nur gelesen und nicht verändert werden.

Die Verwendung eines Globalen Katalogs in einer Domäne veranlasst andere Domänencontroller, die Replikation über diesen durchzuführen. Sind keine GCs in einer Domäne vorhanden, übernimmt ein Domänencontroller diese Aufgabe.

Replikationstopologie

Die *Replikationstopologie* beschreibt die Art und Weise, wie die Domänencontroller ihre Daten synchronisieren. Die Replikationstopologie wird automatisch erstellt und angepasst, wenn sich etwas an der Konfiguration der Domänencontroller ändert.
Ein Domänencontroller versucht möglichst zwei Verbindungen zu anderen Domänencontrollern aufzubauen, damit beim Ausfall eines Servers die Synchronisation trotzdem noch funktioniert. Eine Ausnahme sind Verbindungen zwischen Standorten, die nicht automatisch erstellt werden, sondern manuell als Standortverknüpfung eingerichtet werden müssen. Dabei werden Parameter, wie Kosten, Geschwindigkeit und Zeit der Replikation angegeben, auf deren Basis die Replikationstopologie angepasst wird.

Zusammenfassung

Das Active Directory ist ein neuer Verzeichnisdienst unter Windows 2000, der von vielen Diensten und Programmen verwendet wird. Die wichtigste Rolle ist die Speicherung und Verwaltung der Domänendaten und der Domänenstruktur. Die Verwendung von vorhandenen Internetprotokollen erleichtert die Anbindung von Programmen an diesen Verzeichnisdienst. Der Einsatz von einem hierarchischen Namensraum für die Domänenstruktur und die Unterscheidung zwischen Standorten und Domänen, wird der Anforderung nach verteilten Systemen gerecht.

2.1.4 Encrypting File System (EFS)

Das *verschlüsselnde Dateisystem* unter Windows 2000 mit NTFS5 basiert auf einer Verschlüsselung mit öffentlichen Schlüsseln. EFS ist als Systemdienst integriert und kann mit einer Infrastruktur öffentlicher Schlüssel (Public Key Infrastructure - PKI), falls vorhanden, zusammenarbeiten, um die Schlüsselverwaltung zu regeln, sie ist für die Funktionsweise aber nicht zwingend erforderlich. Bei der erstmaligen Verwendung von EFS wird der Benutzer *Wiederherstellungsagent* (Data Recovery Agent – DRA) angelegt, der es ermöglicht, Dateien zu entschlüsseln, auch wenn der Benutzer seinen Schlüssel verloren oder das Unternehmen verlassen hat. Der Benutzer bekommt durch die Verwendung des Prinzips der öffentlichen Schlüssel vom Ver- und Entschlüsselungsvorgang, außer einem geringen Zeitunterschied zum normalen Dateizugriff, nichts mit, die Dateien verhalten sich für ihn wie normale, unverschlüsselte Dateien. Das System ist dadurch für den Benutzer transparent.

Als Verschlüsselungsalgorithmus wird DESX, eine Erweiterung des DES[14]-Standards, verwendet. Seine Schlüssellänge beträgt 120 Bit und im Gegensatz zu DES wird jeder Block dreimal mit verschiedenen Schlüsseln verarbeitet. Dabei wird der erste Schlüssel mit XOR angewendet, der zweite mit dem DES-Algorithmus und der dritte wieder mit XOR. Die Entschlüsselung geschieht genau umgekehrt. Dieser Algorithmus ist relativ sicher und um einiges sicherer als DES. Das EFS verschlüsselt immer in 512 Byte großen Blocks.

Eine Bedingung für das Funktionieren von EFS ist die Existenz eines Wiederherstellungsagenten (DRA). Wird zum ersten Mal auf einem System eine Datei verschlüsselt, wird dieser Benutzer bei Nichtvorhandensein angelegt. Der Wiederherstellungsagent ist im Besitz eines Wiederherstellungszertifikats und eines Schlüsselpaares aus öffentlichem und privatem Schlüssel, mit dessen Hilfe er Dateien im System entschlüsseln darf, weshalb auch in jeder verschlüsselten Datei sein öffentlicher Schlüssel stehen muss. Die Existenz dieses Agenten ist in Windows 2000 so wichtig, dass ohne ihn keine Verschlüsselung stattfindet, bzw. die Verschlüsselung vom System abgelehnt wird. In einem Einzelplatzsystem wird dem Administrator ein Wiederherstellungsschlüssel zugeteilt und dieser erfüllt die Funktionalität des Wiederherstellungsagenten. Es gibt auch die Möglichkeit mehrere Wiederherstellungsagenten anzulegen, hierbei besitzt jeder ein Schlüsselpaar und ein Zertifikat und ihre öffentlichen Schlüssel stehen dann in jeder verschlüsselten Datei, damit jeder von ihnen getrennt von den anderen die Datei entschlüsseln kann.

Die folgende Abbildung beschreibt den Ablauf der Verschlüsselung einer Datei auf Betriebssystemebene, wobei der NTFS-Dateisystemtreiber den wichtigsten Teil übernimmt.

14 Data Encryption Standard

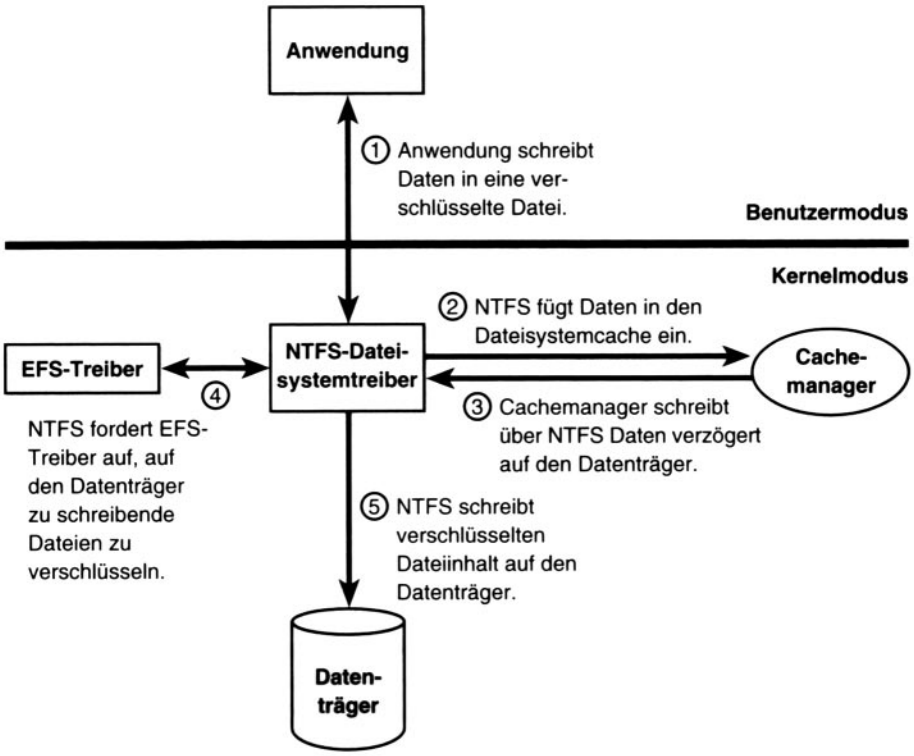

Abbildung 2-4 „EFS-Ablauf" [SOL00]

Funktionsweise

Bei der Verschlüsselung einer Datei wird ein zufällig generierter Schlüssel für die Verschlüsselung der Daten benutzt und dieser *Dateiverschlüsselungsschlüssel* (File Encryption Key – FEK) wird dann mit dem privaten Schlüssel des Besitzers verschlüsselt und mit der Datei abgespeichert. Dies geschieht in einem zusätzlichen Attribut der Datei, das *$Logged_Utility_Stream* heißt. Hier wird das *Data Decryption Field* (DDF), in dem der verschlüsselte FEK steht, und das *Data Recovery Field* (DRF), in dem sich der öffentliche Schlüssel des oder der Wiederherstellungsagenten befindet, eingetragen, damit ein solcher in die Lage versetzt wird, im Notfall die Datei zu entschlüsseln.

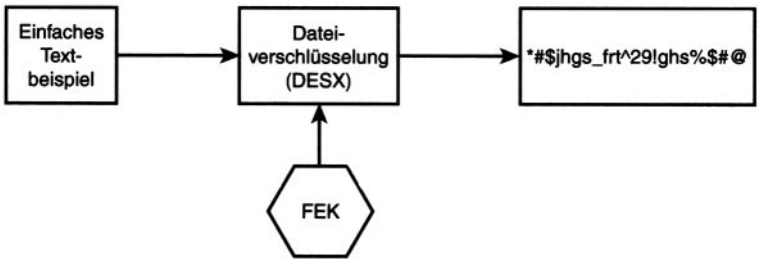

Abbildung 2-5 „EFS Verschlüsselung" [LEE00]

Zur Entschlüsselung wird im DDF nach dem Besitzer (Verschlüsseler) der Datei gesucht und dann mit seinem privaten Schlüssel der FEK aus dem DDF entschlüsselt. Mit diesem FEK kann danach die Datei entschlüsselt und an die anfordernde Anwendung weitergegeben werden. Die entschlüsselte Datei wird im Objektcache und nicht in einer temporären Datei abgelegt, was die Sicherheit erhöht.

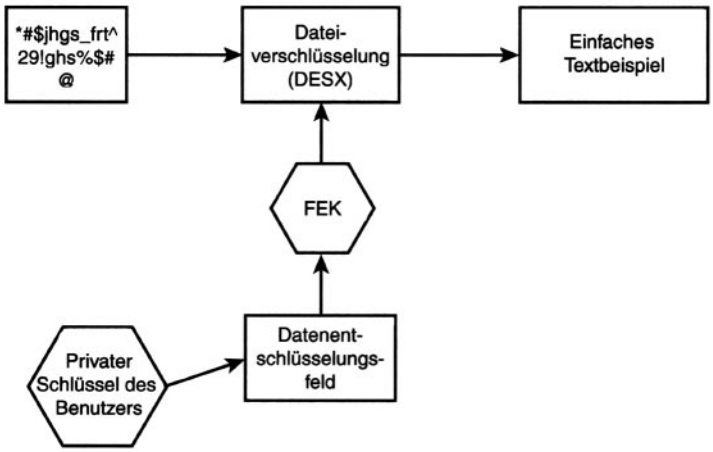

Abbildung 2-6 „EFS Entschlüsselungsdiagramm" [LEE00]

Bei der Entschlüsselung durch den Wiederherstellungsagenten wird mit Hilfe seines privaten Schlüssels und dem DRF der FEK entschlüsselt und anschließend die Datei. Der Vorgang ist somit nahezu der gleiche und da sein Schlüssel vollkommen getrennt von dem des Benutzers ist, wird die Sicherheit des privaten Schlüssels des Benutzers nicht kompromittiert.

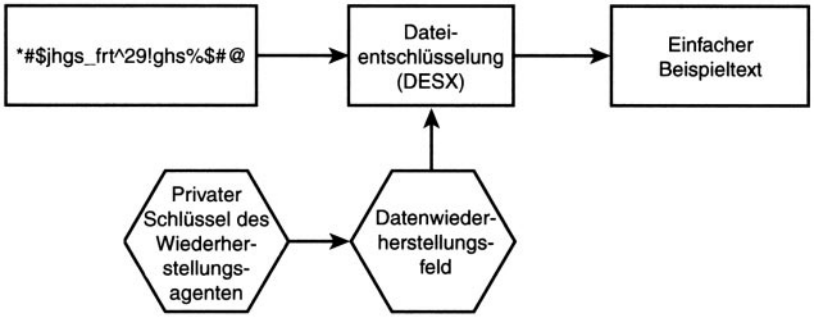

Abbildung 2-7 „Ablauf der EFS-Wiederherstellung" [LEE00]

Bei der Verschlüsselung einer Datei auf einem Server führt der Server die Verschlüsselung durch und braucht deshalb ein Zugriffstoken des Benutzers und den FEK. Die Zugriffsberechtigungen werden über Kerberos (siehe Kapitel 2.1.6) geregelt. Das gleiche Prinzip wird auch bei der Entschlüsselung auf einem Server angewendet.

Die Verschlüsselung kann im Windows-Explorer durch einen Klick mit der rechten Maustaste auf eine Datei oder einen Ordner unter Eigenschaften mit der Schaltfläche Erweiterte Attribute mit Hilfe des Punktes ‚Inhalt verschlüsseln, um Daten zu schützen' aktiviert werden. Alternativ kann man das Befehlszeilendienstprogramm ‚*cipher.exe*' benutzen.

Nutzen mehrere Benutzer eine verschlüsselte Datei, so wird der FEK mit jedem öffentlichen Schlüssel jedes Benutzers verschlüsselt und die verschlüsselten FEKs der Benutzer mit der Datei abgespeichert. Möchte nun einer der Benutzer auf die Datei zugreifen, wird sein verschlüsselter FEK mit seinem privaten Schlüssel entschlüsselt und mit diesem dann die Datei.

Eigenarten

Das System besitzt jedoch einige Eigenarten, die man kennen sollte. Verschlüsselt man beispielsweise einen Ordner, wird nicht der Ordner verschlüsselt, sondern nur die enthaltenen Dateien. Dabei bekommt der Ordner das Attribut FILE_ATTRIBUTE_ENCRYPTED und dadurch werden auch neue oder hinzugefügte Dateien automatisch verschlüsselt. Ordner, die in einem solchen Ordner erstellt werden, erhalten das Attribut ebenfalls und verschlüsseln neu erstellte Dateien. Somit vererben sich die Attribute weiter.

Des Weiteren können mit EFS verschlüsselte Dateien nicht mit der Windows 2000 internen Dateikomprimierung komprimiert oder im Netzwerk freigegeben werden.

Das System erlaubt nicht, Dateien im Root- und im WINNT-Verzeichnis zu verschlüsseln, da EFS beim Systemstart nicht zur Verfügung steht und die Start- oder Systemdateien, die beim Booten des Rechners erforderlich sind, dann nicht gelesen werden könnten.

Bei dem Versuch eine Datei auf einer NTFS4-Partition, also einer Partition, die mit Windows NT 4.0 erstellt wurde und die eventuell im System vorhanden sein kann, zu verschlüsseln, wird diese Partition gleich für eine Konvertierung in eine NTFS5-Partition vorgemerkt, ohne dass man vielleicht von NTFS4 auf NTFS5 umsteigen möchte.

Backups von Datenträgern mit verschlüsselten Dateien können nur mit Windows 2000 konformen Backup-Programmen durchgeführt werden, da bei Kopieraktionen auf nicht-NTFS5-Datenträger die Verschlüsselung verloren gehen kann. Diese nutzen die von Windows 2000 bereitgestellten EFS-APIs OpenEncryptedFileRaw, ReadEncryptedFileRaw, WriteEncryptedFileRaw und CloseEncryptedFileRaw. Mit Hilfe dieser Funktionen wird der verschlüsselte Inhalt der Datei getrennt von den EFS-Attributen in der Datei gesichert und sie können beim Zurücksichern auch wieder zusammengesetzt werden.

Mit dem Utility ‚efsinfo.exe' aus dem Windows 2000 Resource Kit ist es möglich in einer verschlüsselten Datei nachzuschauen, wer der Besitzer ist und welche Wiederherstellungsagenten die Datei wiederherstellen können. Dies kann von großem Nutzen sein.

Fazit

EFS ist eine sehr sinnvolle Erweiterung für tragbare Computer oder bei Festplattendiebstahl. Wird die Festplatte mit verschlüsselten Daten in einen anderen Rechner eingebaut, sind nun nicht mehr wie früher bei Windows NT 4.0 Partitionen sämtliche Daten sichtbar, sondern weiterhin nur die unverschlüsselten. Außerdem ist es nicht mehr möglich einen Rechner mittels Disketten mit speziellen Tools zu booten und die verschlüsselten Dateien auf dem Datenträger zu sehen.

2.1.5 Netzwerk

Windows 2000 wurde von Anfang an als Netzwerkbetriebssystem konzipiert. Eine Netzwerksoftware besteht generell aus vier Basistypen, den Diensten, den APIs, den Protokollen und den Netzwerkadaptergerätetreibern. Diese bilden zusammen den Netzwerkstapel. Es ist für Fremdhersteller unter Nutzung dieser vier Basistypen möglich, die Netzwerkfähigkeiten von Windows 2000 durch eigene Implementationen zu erweitern.

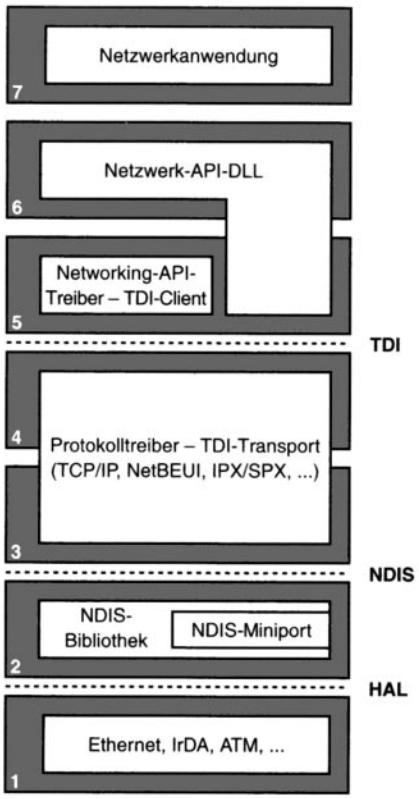

Abbildung 2-8 „OSI-Modell und Windows 2000-Netzwerkkomponenten" [SOL00]

Diese Abbildung zeigt den Aufbau der Komponenten für den Netzwerkbetrieb und schafft eine Übersicht zu den Parallelen des OSI-Referenzmodells[15] der ISO[16]. Wie in der Abbildung auffällt, entspricht das OSI-Modell nicht ganz der Implementation, die Microsoft in Windows 2000 gewählt hat.

15 OSI steht für Open Systems Interconnection

16 International Organization for Standardization

Netzwerkkomponenten

Das Netzwerk besteht aus folgenden Komponenten:

- *Netzwerk-APIs* ermöglichen Anwendungen miteinander zu kommunizieren, ohne auf die Protokolle, etc. eingehen zu müssen. Sie können im Benutzer- oder im gemischten Benutzer- und Kernelmodus programmiert sein. Man kann sie auch als Programmierschnittstellen für Netzwerksoftware bezeichnen.
- *TDI-Clients* (Transport Driver Interface) sind Kernelmodusgerätetreiber und senden E/A-Anforderungspakete *(IRPs – I/O Request Packets)* an die Protokolltreiber, die nach dem Windows 2000 Transport Driver Interface formatiert sind.
- *TDI-Transporte*, auch Transporte, NDIS-Protokolltreiber *(Network Driver Interface Specification)* und Protokolltreiber genannt, sind Kernelmodus-Protokolltreiber. Sie erhalten IRPs von den TDI-Clients und verarbeiten die enthaltenen Anforderungen. Dies geschieht transparent für die Anwendungen, da protokollspezifische Header (z.B. TCP, UDP, IPX) sowie Segmentierung, Reassemblierung und andere Funktionen von ihnen durchgeführt werden.
- *NDIS-Bibliothek* (Ndis.sys) als Kapselung für Adaptertreiber und exportiert Funktionen, die beispielsweise von den TDI-Transporten benutzt werden.
- *NDIS-Miniport-Treiber* sind Kernelmodustreiber und dienen der Kommunikation zwischen Netzwerkadaptern und TDI-Transporten, verarbeiten aber keine IRPs, sondern rufen die NDIS-Bibliothek auf, die Zeiger auf Funktionen enthält, mit denen die IRPs an die TDI-Transporte weitergeleitet werden.

Netzwerk-APIs

In Windows 2000 sind mehrere Netzwerk-APIs implementiert, um auch ältere Anwendungen und Industriestandards zu unterstützen. Zu diesen gehören: NamedPipes, Mailslots, Windows-Sockets (Winsock), Remoteprozeduraufruf (RPC – Remote Procedure Call), CIFS (Common Internet File System) und NetBIOS. Es gibt einige weitere, die auf diesen aufbauen. Der I/O Manager kümmert sich beispielsweise um Disk- und Netzwerk-Vorgänge, er eröffnet dem Benutzermodus einige der hier genannten APIs.

Die folgende Abbildung zeigt die Netzwerkarchtitektur von Windows 2000.

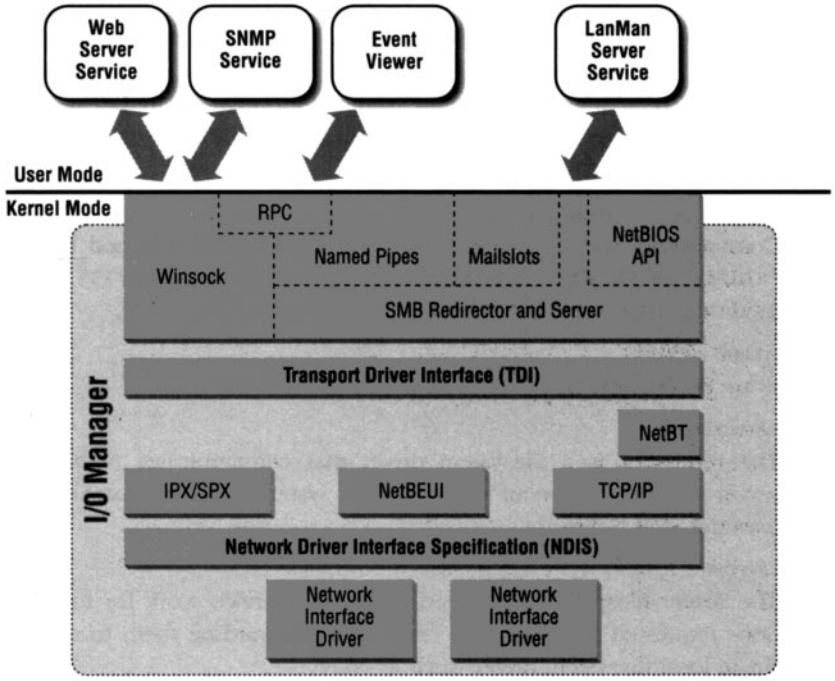

Abbildung 2-9 „The Windows NT networking architecture" [NOR00]

NamedPipes bieten eine zuverlässige Client-Server-Kommunikation für Nachrichten und Daten (Nachrichten- oder Bytemodus), können in der Anzahl der maximal verbundenen Clients beschränkt und im uni- und bidirektionalen Betrieb betrieben werden. Sie arbeiten mit den normalen Win32-Funktionen ReadFile und WriteFile. Zusätzlich bietet die Funktion *ImpersonateNamedPipeClient* die Möglichkeit für den Server, die Identität des Clients anzunehmen *(Identitätswechsel)*. Einige Systemkomponenten von Windows 2000 verwenden NamedPipes zur Kommunikation.

Mailslots ermöglichen den Betrieb von nicht zuverlässigen, unidirektionalen Broadcastmechanismen, die beispielsweise für die Verbreitung des Serverzeitsignals im Netzwerk benutzt werden können.

Windows-Sockets (Winsock) ist die Microsoft-Implementierung des BSD-Sockets (Berkeley Software Distribution), bietet fast alle ihrer Funktionen und noch einige Microsoft-spezifische Verbesserungen. In Windows 2000 wird Winsock in der Version 2.2 eingesetzt, welches in den anderen Windows Versionen enthalten oder als Add-On verfügbar ist. Es unterstützt QoS (Quality of Service), Multipointnachrichten (Nachrichten gleichzeitig an mehrere Empfänger), Erweiterbarkeit um Protokolle, die nicht mit Windows 2000 ausgeliefert wurden, und Portierungsmöglichkeiten für UNIX-Netzwerkanwendungen, die für BSD-Sockets geschrieben wurden. Die Arbeitsweise läuft nach einem festen Schema ab: Es wird ein Socket erstellt, das an einen lokalen Computer gebunden werden muss. Da Winsock protokollunabhängig ist, muss für jedes installierte Protokoll eine Adresse gebunden werden. Es gibt die verbindunglose und die verbindungsorientierte Socket-Operation. Bei der zweiten wird auf dem Server ein Socket mit einer ‚listen' (abhören) Funktion ausgeführt. Bei einer Anfrage mit Hilfe der Funktion ‚connect' unter Angabe der Remoteadresse

wird über ‚accept' die Verbindung aufgebaut und es können mit ‚recv' und ‚send' Daten empfangen und gesendet werden. Bei der verbindungslosen Variante werden einfach Nachrichten gesendet und empfangen, in denen die Remoteadresse angegeben ist. Der missglückte Empfang einer Nachricht wird durch das Senden eines Fehlercodes angezeigt. Nach dem Verbindungsaufbau und dem Binden der Adresse sind die beiden Arten nicht mehr voneinander zu unterscheiden. Durch die Möglichkeit der asynchronen Kommunikation über Winsock, ist die Möglichkeit gegeben, auf einfache Art und Weise Anwendungen zu entwickeln, da diese nicht Multithreading oder Synchronisierung unterstützen können müssen, um über das Netzwerk kommunizieren oder Benutzereingaben verarbeiten zu können. Zusätzliche Microsoft-Funktionen sind z.B. ‚AcceptEx' und ‚TransmitFile', die in IIS 5 zur Leistungssteigerung eingesetzt werden. Die erste ermöglicht eine Variante von accept, bei der nur eine Winsock-Funktion zum Verbindungsaufbau ausgeführt werden muss (und nicht mehrere wie bei accept) und die zweite kann verwendet werden, um Dateien (hier z.B. Webseiten) direkt vom Windows 2000-Cachemanager, also direkt aus dem Dateisystem, senden zu lassen. Diesen Vorgang nennt man Zero-Copy-Kommunikation, da der Server die Datei nicht bearbeiten muss, um sie senden zu können. TransmitFile bietet außerdem die Möglichkeit, Dateien Daten voranzustellen oder anzuhängen. WinSock ist um TDIs von Fremdherstellern erweiterbar, die nach der Registrierung ebenfalls die erläuterten Funktionen verwenden können.

Remoteprozeduraufruf (RPC – Remote Procedure Call) ist ein Netzwerkprogrammierstandard, der auf anderen Netzwerk-APIs wie NamedPipes oder Winsock aufbaut, um Programmierern die Entwicklung von dezentralen Anwendungen zu erleichtern und ihnen den Umgang mit Netzwerkprotokollen oder Netzwerkfehlern zu ersparen. Netzwerkoperationen werden prozedural gesehen, wobei Prozeduren teils auf dem lokalen Rechner und teils auf Remotesystemen ausgeführt werden können. Beispielsweise kann man arithmetische Berechnungen auf eine evtl. vorhandene Cray auslagern, sich die Ergebnisse zurückgeben lassen und damit weiterarbeiten. RPC-Software bearbeitet auch das Warten und Einbinden der Ergebnisse automatisch, somit müssen die Netzwerkoperationen hierfür von den Programmierern nicht geschrieben werden. Ein wichtiger Punkt bei der Ausführung von Prozeduren auf Remoterechnern ist das *Marshalling*, das bewirkt, dass Dateien und Verweise, die für die Berechnung auf dem anderen Rechner erforderlich sind, aufgelöst und mitgeschickt werden. Der Remoterechner führt dann bei Erhalt der Prozeduren das *Unmarshalling* durch, das die nötigen Daten auf dem Rechner zur Verfügung stellt. Dieses Verfahren ist ein synchroner RPC. Es gibt auch asynchrone RPCs unter Windows 2000, bei denen Anwendungen Remote-Funktionen starten können und ohne auf die Ergebnisse warten zu müssen weitere Funktionen starten können. Die meisten Windows-Netzwerkdienste sind RPC-Anwendungen und können daher z.B. auf Servern Freigaben auflisten, Dateien öffnen oder in Druckerwarteschlangen schreiben. Dies geschieht natürlich unter Bewahrung der Sicherheitsrichtlinien. Über SSPs *(Security Support Provider)* kann auch die RPC-Kommunikation verschlüsselt werden. Windows integriert einige SSPs: Kerberos, Secure Channel (SChannel), Secure Sockets Layer (SSL),etc. Als Standard werden für die Kommunikation NamedPipes mit ihrer integrierten Sicherheit verwendet.

DCOM (Distributed Component Object Model) benutzt RPCs. Es gibt zwei Möglichkeiten hierfür:
1. RPC over SMB: diese benutzt SMB NamedPipes für den Transport der RPCs und wird z.B. von Server Manager, Benutzer Manager, Performance Monitor, Ereignisanzeige und NT-Domains verwendet.
2. RPC über Windows Sockets: die Kommunikation wird über dynamische, hohe Ports (<1023) und RPC-Portmapper-Dienste tcp/135 und udp/135 aufgebaut. Diese Variante wird oft von DCOM Anwendungen genutzt, da man DCOM über ‚dcomcnfg.exe' eine bestimmt Portzahl zuweisen kann.

Das *Common Internet File System* (CIFS) ermöglicht Datei- und Druckerfreigabe und ist eine Erweiterung des SMB-Protokolls (Server Message Block). Es ermöglicht auch die Dateidienste von Unix oder Apple für Windows-Rechner zugänglich zu machen.

NetBIOS (Network Basic Input/Output System) ist eine ältere Programmier-API, Microsoft rät Entwicklern jedoch von ihrer Benutzung ab und empfiehlt NamedPipes oder Winsock, da diese flexibler und portabler sind. Die Protokolle TCP/IP, NetBEUI *(NetBIOS Extended User Interface)* und IPX/SPX unterstützen NetBIOS unter Windows 2000 und mit NetBT (NetBIOS over TCP/IP) wird NetBIOS routingfähig . Bei der Installation von Windows 2000 ist die Angabe eines NetBIOS-Namens für den Rechner Pflicht. Allerdings werden Computernamen zuerst über DNS registriert und erst wenn die DNS-Namensauflösung scheitert, wird auf NetBIOS-Namen zurückgegriffen. Die Pflege zwischen TCP/IP-Adressen und NetBIOS-Namen übernimmt WINS (*Windows Internet Name Service*). Falls WINS nicht installiert ist, wird Namensbroadcasting verwendet, um Namen im Windows-Netzwerk aufzulösen. Sind mehrere Netzwerkkarten in einem Rechner installiert, werden für sie LANAs (LAN-Adapternummern) vergeben und diesen NetBIOS-Namen zugewiesen. Auf einem Server führt NetBIOS den Befehl ‚listen' aus, um auf Clientverbindungen zu warten. Auch hier gibt es verbindungslose Kommunikation, bei der der Server einfach Nachrichten liest, ohne Verbindungen aufzubauen und die Clients geben beim Senden den NetBIOS-Namen des Servers an. Alternativ gibt es die verbindungsorientierte Kommunikation, die man auch als Sitzung bezeichnet. Bei dieser Variante wird eine Verbindung aufgebaut und Client und Server tauschen Daten mit Hilfe von NetBIOS-Funktionen aus.

Mit Windows 2000 werden folgende Protokolltreiber ausgeliefert:

- *TCP/IP* (Transmission Control Protocol / Internet Protocol) wird als einziges Protokoll standardmäßig auf Windows 2000 Rechnern installiert. Es ist das bevorzugte Protokoll in Windows 2000, bietet Routingfähigkeit und gute Leistung im Wide Area Network.
- *NetBEUI* ist nicht routingfähig und auf Wide Area Networks nicht performant. Es arbeitet eng mit der NetBIOS-API zusammen, verwendet das Protokollformat NetBIOS Frame (NBF) und dient nur der Unterstützung älterer Windows Systeme (z.B. Windows NT 4.0).
- *NWLink* besteht aus den Novell Protokollen IPX und SPX und wird bei Bedarf für die Zusammenarbeit mit Novell-Servern installiert.
- *DLC* ist ein einfaches Protokoll, das Netzwerk-APIs nicht verwenden können, sondern welches direkt mit Geräten verwendet werden muß. Es wird von einigen IBM-Großrechnern sowie Hewlett-Packard Netzwerkdruckern eingesetzt.

- *AppleTalk* ist zuständig für Datei-und Druckdienste für Apple Macintosh Rechner auf Windows 2000 Servern.

NDIS-Treiber (Network Driver Interface Specification) wurden 1989 von Microsoft und 3com entwickelt und sollen geräteunabhängige Kommunikation zwischen Protokolltreibern und Netzwerkadaptertreibern ermöglichen. Treiber dieser Art werden NDIS-Treiber oder NDIS-Miniport-Treiber genannt. In Windows 2000 ist NDIS 5 implementiert. Die NDIS-Bibliothek empfängt IRPs von den TDI-Servern und übersetzt sie für die NDIS-Treiber. Dadurch „sieht" der NDIS-Treiber die IRPs gar nicht und er muss sich auch nicht um weitere Anfragen, als die, die er momentan bearbeitet, kümmern, weil auch das die NDIS-Bibliothek übernimmt. Insofern wird den Herstellern die Implementation der Treiber wesentlich erleichtert. Außerdem bietet NDIS 5 noch einige weitere Funktionen:

1. NDIS-Treiber können kenntlich machen, ob ihr Netzwerkmedium aktiv ist oder nicht. In der Windows-Taskleiste wird das durch ein Symbol angezeigt. Dies wird auch von anderen Protokollen genutzt.
2. TCP/IP-Aufgabenentlastung kann beispielsweise Ipsec-Verschlüsselung in Hardware auf der Netzwerkkarte ausführen lassen, um die Rechnerressourcen zu schonen.
3. Schnelle Paketweitergabe erlaubt Pakete, die für andere Rechner bestimmt sind, direkt weiterzuleiten, ohne sie der CPU zu übergeben.
4. Wake-On-LAN ermöglicht, einen Rechner durch ein Paket vom Netzwerk aus zu „wecken", also zu booten oder aus dem Standby-Modus erwachen zu lassen.
5. Verbindungsorientiertes NDIS erlaubt Verbindungen mit ATM-Geräten (Asynchronous Transfer Mode), die in Windows 2000 erstmalig unterstützt werden, wobei Pakete nur über aufgebaute Netzwerkverbindungen gesendet werden, statt sie einfach ins Netzwerkmedium zu senden.

NDIS-Zwischentreiber liegen zwischen dem NDIS-Treiber und dem TDI-Transport und können dadurch den gesamten Netzwerkverkehr auf einem System einsehen. Für den NDIS-Treiber sieht er wie der TDI-Transport aus und umgekehrt. Sie eröffnen zum Beispiel die Möglichkeiten des Netzwerkmonitors, eines Dienstprogrammes von Windows 2000 Server, mit dem man sich alle Pakete, die durch den eigenen Rechner fließen, anschauen kann.

Bindungen ermöglichen die Kommunikation mit Komponenten in angrenzenden Ebenen im Protokollstapel. Man kann hiermit z.B. einen Dienst an ein Netzwerkprotokoll binden und die anderen verbieten oder einer Netzwerkkarte im Gerät nur ein Netzwerkprotokoll ermöglichen. Somit kann man beispielsweise TCP/IP auf Netzwerkkarte1 ausschließlich ermöglichen und NetBEUI auf Netzwerkkarte2.

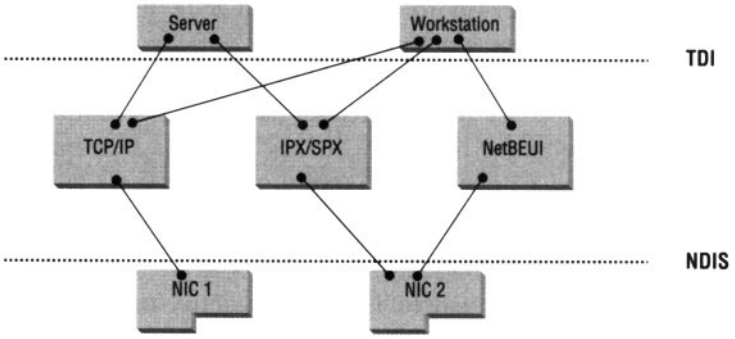

Abbildung 2-10 „Example of bindings in the Windows network architecture" [NOR00]

2.1.6 Kerberos v5

Kerberos ist ein Protokoll zur Netzwerkauthentifizierung und es wurde in den 80er Jahren am Massachusetts Institute of Technology (MIT) mit dem Ziel entwickelt, eine starke Authentifizierungsmethode für Client/Server-Applikationen zu bieten.

Das Protokoll beinhaltet drei Komponenten: Client/Applikation, Netzwerkressource und *Key Distribution Center* (KDC), die für den sicheren Zugriff auf Netzwerkressourcen sorgen. Dafür werden geteilte geheime Schlüssel benutzt. Die Kommunikationspartner benutzen kein Passwort, sondern gemeinsame Schlüssel nach dem Public-Key-Verfahren.

In Windows 2000 ist die aktuelle Version 5 von Kerberos implementiert und als standardmäßiger Authentifizierungsmechanismus für Domänenzugriffe konfiguriert. Es ersetzt NTLM als primären Authentifizierungsdienst, läuft auf allen Windows 2000 Domänencontrollern und alle Windows 2000 Server- und Client-Versionen stellen einen Kerberos-Client zur Verfügung.

Kerberos benutzt so genannte *Tickets* um die Authentizität eines Benutzers zu überprüfen. Der Benutzer erhält bei erfolgreicher Anmeldung ein Ticket und dieses wird verschlüsselt im lokalen System gespeichert. Für jeden Dienst und jeden Zugriff auf diesen Dienst müssen diese Tickets vorgezeigt werden, diese Aktionen bekommt der Benutzer jedoch nicht mit, da sie automatisch im Hintergrund und somit transparent ablaufen.

Bei der Anmeldung an einer Domäne fordert der Benutzer den Zugang zum *Ticket Granting Service* (TGS) der Domäne an und erhält bei erfolgreicher Authentifizierung durch das Key Distribution Center (KDC) ein Ticket.

Das Key Distribution Center verwendet Active Directory (siehe Kapitel 2.1.3) als Datenbank für die Benutzerinformationen. Active Directory läuft als Dienst auf allen Windows 2000 Domänencontrollern und stellt folgende zwei Dienste zur Verfügung:

- Den *Authentifizierungsdienst* (Authentication Service - AS): dieser authentifiziert Benutzer und stellt Ticket-Granting Tickets (TGTs) aus, die vom Client zum Anfordern von Sitzungstickets benötigt werden.

- Den *Ticket-Granting Service* (TGS): dieser vergibt Sitzungstickets für Netzwerkdienste, die auf einem ausgestellten TGT basieren.

Nach erfolgter Authentifizierung über den AS beim KDC, der die Anmeldeinformationen mit den Daten des Benutzerkontos in Active Directory vergleicht und daraufhin ein TGT ausstellt, darf der Client Sitzungstickets anfordern. Das TGT wird verschlüsselt auf dem lokalen System gespeichert und hat eine standardmäßige Lebensdauer von zehn Stunden. Möchte der Benutzer eine neue Netzwerkressource nutzen, sendet er sein TGT an den TGS und fordert für diesen Dienst ein Sitzungsticket an, das dann im *Ticket-Cache* gespeichert wird und für spätere Zugriffe wieder verwendet wird. Nun sendet er das Sitzungsticket an den Netzwerkdienst und erhält Zugriff. Bei jedem Zugriff auf einen Netzwerkdienst wird zuerst im Ticket-Cache nach einem für diesen Dienst gültigen Ticket gesucht. Ist das Ticket abgelaufen oder nicht vorhanden, muss ein neues beim TGS angefordert werden.

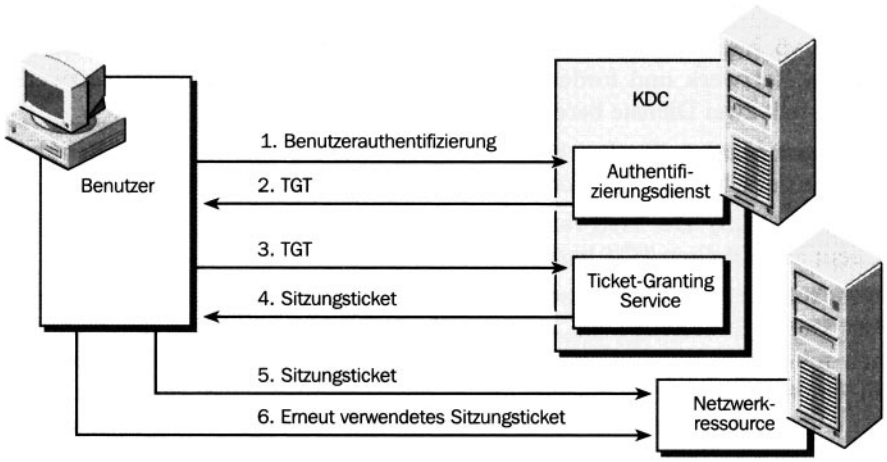

Abbildung 2-11 „Ablauf der Authentifizierung mit Kerberos v5" [ISS00]

Ticket-Details

Teile des Tickets sind mit einem geteilten geheimen Schlüssel verschlüsselt, den nur der Benutzer und der Domänen-Controller kennen. Die anderen Teile des Tickets werden mit einem Schlüssel verschlüsselt, den die Netzwerkressource und der Domänen-Controller teilen. Hierdurch kann jeder Beteiligte seinen Teil des Tickets lesen und seine Identität ist bestätigt. Ein geringer Teil ist unverschlüsselt und enthält die Header-Informationen.

Der unverschlüsselte Teil des Tickets enthält:

- die Versionsnummer des Ticketformats
- den Namen der Domäne, die das Ticket erstellt hat
- den Servernamen, für den es gültig ist

Der restliche Teil des Tickets ist durch den geheimen Schlüssel des Servers verschlüsselt und enthält:

- den von Client und Server gemeinsam genutzten Sitzungsschlüssel für sichere Übertragungen
- den Namen der Domäne des Clients
- den Clientnamen
- den Zeitstempel der ersten erfolgten Anmeldung am TGS für dieses Ticket
- die Lebensdauer des Tickets

Zusätzlich gibt es Kerberos-Ticket-Flags, von denen hier die wichtigsten erwähnt werden sollen:

- Forwardable/Forwardable Tickets
- Renewable Tickets
- Proxy Tickets

Mit Hilfe von *Forwardable Tickets* ist es möglich, Informationen zwischen Front-End- und Back-End-Servern auszutauschen. Dabei wird vom KDC ein Ticket für den Front-End-Server ausgestellt, mit dem er den Namen des Clients benutzen, die Information holen und diese dann wieder an den Client zurücksenden kann. Somit wird der Abruf der Tickets delegiert. Für die so genannte Delegierung der Authentifizierung teilt der Client dem KDC mit, dass der Front-End-Server für ihn agieren soll und der Server führt dann einen Identitätswechsel durch. Dieses kann auf zwei Arten geschehen. Entweder erhält der Client ein Ticket für den Back-End-Server und gibt dieses dann dem Front-End-Server, hierbei handelt es sich um ein *Proxy-Ticket*, das allerdings den Namen des Back-End-Servers kennen muss; oder der Client gibt dem Front-End-Server ein TGT, das falls nötig für die Erstellung von Sitzungstickets benutzt wird und die Weiterleitung der Informationen an den Client ermöglicht. Im zweiten Fall handelt es sich um Forwardable Tickets. Welche dieser beiden Formen benutzt wird, hängt von den Einstellungen der Administrationsrichtlinien ab.

Läuft ein Ticket während der Benutzung ab, wird die Verbindung nicht unterbrochen, für die nächste Anmeldung bei dem benutzten Dienst muss jedoch ein neues Ticket angefordert werden. Benutzer können während des Gültigkeitszeitraums eines Tickets so oft Verbindungen mit einem Dienst aufbauen wie sie möchten. Ein Sitzungsticket hat normalerweise eine Lebensdauer von zehn Stunden.

Der Ticket-Cache wird beim Abmelden des Benutzers oder Herunterfahren des Rechners gelöscht, so dass die Tickets nicht von anderen abgerufen werden können, er ist ein Bereich des flüchtigen Speichers und wird nie auf der Festplatte ausgelagert. Dieser wird vom *Kerberos Security Support Provider* (SSP) verwaltet, der der *Local Security Authority* (LSA) von Windows 2000 untersteht.

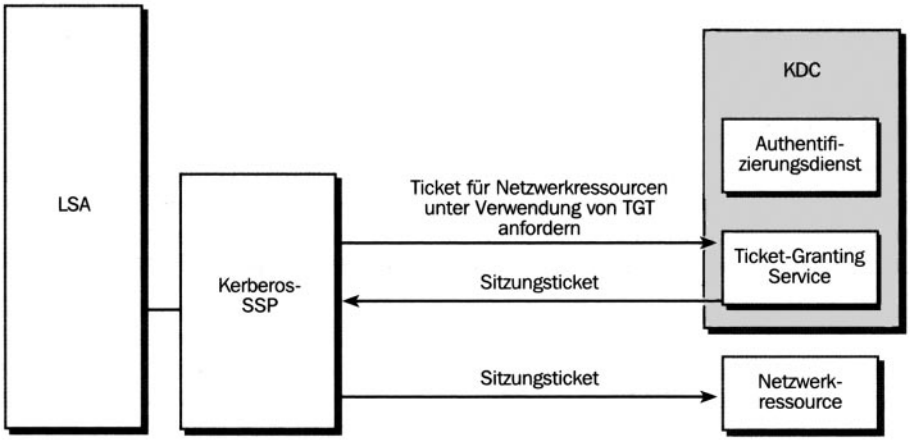

Abbildung 2-12 „Netzwerkauthentifizierung" [ISS00]

Administrationseinstellungen

Kerberos sieht die Einstellung von Richtlinien vor, die nach der Konfiguration für die gesamte Domäne zur Verfügung stehen. Die konfigurierbaren Werte und deren Standardeinstellungen sind Folgende:

- Benutzeranmeldeeinschränkung erzwingen: *JA.* Bei dieser Einstellung wird bei jeder Ticketanforderung eine Überprüfung der Benutzerrechte durch das KDC durchgeführt und es ergibt sich eine höhere Zugriffszeit und erhöhter Netzwerkverkehr.
- Max. Lebensdauer eines Diensttickets: *zehn Stunden.* In diesem Zeitraum wird einem Benutzer bei Vorzeigen des Tickets Zugriff auf eine Ressource gewährt.
- Max. Lebensdauer eines Benutzertickets: *zehn Stunden.* Das TGT darf innerhalb dieses Zeitraums für die Anforderung von Sitzungstickets verwendet werden, danach muss es verlängert oder erneuert werden.
- Max. Lebensdauer eines verlängerten Benutzertickets: *sieben Tage.* Dieser Wert beschreibt die Gültigkeitsdauer eines TGTs, das verlängert wurde.
- Max. Abweichung bei der Synchronisierung der Computeruhr: *fünf Minuten.* Der Zeitunterschied zwischen Client- und Serveruhr darf hier maximal fünf Minuten betragen. Hiermit soll sichergestellt werden, dass unbefugte Benutzer gültige Tickets nicht kopieren und zu einem späteren Zeitpunkt zur Anmeldung benutzen können.

Vorteile von Kerberos für Windows 2000

Laut Microsoft ist ihre Kerberos v5-Implementation vollkommen kompatibel zur Spezifikation der IETF nach [RFC1510] und [RFC1964].
Zu den Vorteilen gegenüber dem NT Lan Manager (NTLM) von Windows NT 4.0 zählen ein schnellerer Sitzungsaufbau, die Delegierung der Authentifizierung, die dem Client ermöglicht einen Server zu autorisieren, seine Identität anzunehmen und sich dadurch an einem zweiten Server anzumelden, wenn man auf einem entfernteren Server Zugriff benötigt und transitive Vertrauenseinstellungen, die zur Vererbung von Vertrauensbeziehungen zwischen mehreren Domänen führen. Zusätzlich ermöglicht Kerberos in Verbindung mit Active Directory ein Single-Sign-On (SSO) in die Windows-2000-Umgebung, bei der man nur eine Anmeldung durchführen muss und weitere

Anmeldungen automatisch abgewickelt werden. Durch die Verwendung der Sitzungstickets wird außerdem der Netzwerkverkehr vermindert, weil nicht mehr so viele Anmeldevorgänge wie bei Windows NT 4.0 nötig sind, bei dem die Netzwerkverbindung nach 15 Minuten Inaktivität eine erneute Authentifizierung erfordert.

2.1.7 Infrastruktur öffentlicher Schlüssel (PKI)

Eine *Infrastruktur öffentlicher Schlüssel* (Public Key Infrastructure – PKI) ermöglicht einen vertraulichen Datenaustausch mit Hilfe von *Authentifizierungsdokumenten* zwischen Client- und Serveranwendungen. Diese Dokumente können nicht erraten werden und sind daher viel sicherer als Passwörter oder ähnliche Authentifizierungsmechanismen. Mit einer PKI wie der in Windows 2000, ist es möglich, Authentifizierungsdokumente selbst zu erstellen und an seine Kommunikationspartner zu verteilen, um diese in die Lage zu versetzen, sich an dem Server, der die Dokumente erstellt hat authentifizieren zu können. Es ist außerdem möglich, die Ausstellung von Authentifizierungsdokumenten an eine *Authentifizierungsstelle* (Certificate Authority – CA) zu delegieren, man muss dann lediglich den eigenen Servern mitteilen, dass sie den Authentifizierungsdokumenten dieser Stellen vertrauen sollen. Erst durch eine PKI wird die einfache Benutzung von Public-Key-Verfahren möglich.

Die Basis hierfür bildet eine asymmetrische Verschlüsselung, die auf Schlüsselpaaren aus öffentlichen und geheimen Schlüsseln beruht. Zu diesem Schlüsselpaar gehört ein *Schlüsselzertifikat*, das von einer CA ausgegeben wird und den öffentlichen Schlüssel mit dem Namen der Entität, beispielsweise des Servers, für einen bestimmten Zeitraum verknüpft. Wenn Entität A Entität B ein Zertifikat vorlegt, erkennt Entität B am Namen, dass es einem seiner Benutzer gehört und weist Entität A den Besitz des privaten Schlüssels des Benutzers nach. Entität A kann in der *Zertifikatsrückziehungsliste* (Certificate Revocation List – CRL) überprüfen, ob das Zertifikat von Entität B gültig oder abgelaufen ist. Nach diesem Vorgang können A und B sicher kommunizieren. Dafür benötigen sie keine dritte Entität wie beispielsweise bei Kerberos das Key Distribution Center (KDC), sondern können sich untereinander authentifizieren.
Hieraus resultiert auch die Möglichkeit zweier Benutzer, untereinander verschlüsselte E-Mails austauschen zu können, ohne eine vermittelnde Entität zu benötigen. Außerdem sind öffentliche Schlüssel meist 1024 Bit lang und somit sehr sicher.

CAs müssen Schlüsselbesitzer eindeutig identifizieren, bevor sie Zertifikate ausstellen, sie müssen Zertifikate einziehen, wenn deren Gültigkeit abgelaufen ist und dafür sorgen, dass ihr eigener privater Zertifizierungsschlüssel geheim bleibt. Eine Dokumentation einer CA ist immer erforderlich und kann teilweise von Kommunikationspartnern oder Partnern eingefordert werden. Sie wird als *Certificate Practice Statement* (CPS) bezeichnet.

Zur Distribution der eigenen Schlüssel an Kommunikationspartner wird ein Dokument mit dem eigenen öffentlichen Schlüssel verschlüsselt und an alle Kommunikationspartner weitergegeben, damit sie mit diesem Schlüssel Daten verschlüsseln und senden können. Den geheimen Schlüssel benötigt man, um diese Daten wieder entschlüsseln zu können. Dieser Schlüssel darf auf keinen Fall weitergegeben oder veröffentlicht werden. Es ist auch möglich, ein Dokument mit dem privaten Schlüssel digital zu signieren. Der Autor kann dann mit dem öffentlichen Schlüssel verifiziert

werden und gleichzeitig ist die Integrität der Daten gesichert, da sich ansonsten die Signatur des Autors verändert hätte.

Der kryptografische Hintergrund hierfür besteht aus dem Zusammenspiel von Vertraulichkeit (Nur berechtigte Benutzer haben Zugriff), Authentifizierung (Nachweis der Identität), Datenintegrität (Identität des Autors ist gewährleistet und Daten sind unverändert) und Fälschungssicherheit (Digitale Signatur elektronischer Dokumente im Sinne einer Unterschrift). Ein weiterer wichtiger Punkt ist die Beweisbarkeit einer Transaktion (non-repudiation), durch die ein Transaktionspartner nicht mehr abstreiten kann, dass die Transaktion stattgefunden hat.

PKI-Funktionen in Windows 2000

Windows 2000 ist in der Lage Zertifikate auszustellen und somit die Grundlagen für eine PKI zu legen. Da sich Microsoft hier an Industriestandards gehalten hat, ist es möglich, mit Fremdsoftware, die öffentliche Schlüssel benutzt, zu kommunizieren und mit fremden Zertifikatsdiensten, wie beispielsweise VeriSign[17], zusammenzuarbeiten.

Mit Windows 2000 sind folgende PKI-Funktionen möglich:

- Interne Anwendungen und Dienste, die bereits mit öffentlichen Schlüsseln arbeiten: Internet Information Server, Internet Explorer, Outlook Express und Outlook, verschlüsselndes Dateisystem (EFS), IPSec und die Verwendung von Smartcards
- Veröffentlichung von Zertifikaten und Zertifikatsrückziehungslisten mit Active Directory
- Erzeugung von Zertifikaten und Einführung einer PKI
- Smartcard-Unterstützung für kryptografische Transaktionen
- Teilnahme an bereits im Internet bestehenden PKIs durch in Windows 2000 enthaltene Zertifikate kommerzieller Zertifizierungsstellen
- Administration der Richtlinien öffentlicher Schlüssel in den Gruppenrichtlinien

Die Kommunikation mit anderen Produkten wird durch implementierte Industriestandards wie X.509, LDAP (Lightweight Directory Access Protocol), SSL (Secure Sockets Layer) / TLS (Transport Layer Security), S/MIME (Secure Multipurpose Internet Mail Extension), IPSec und der Erweiterung von Kerberos um öffentliche Schlüssel ermöglicht.

Es kann in Windows 2000 auch mehrere CAs geben, die dann Vertrauensbeziehungen untereinander folgen, wobei die untergeordnete Stelle, die Tochter-CA, ihr Zertifikat von der übergeordneten CA bezieht. Benutzer, die einer übergeordneten CA vertrauen, vertrauen auch automatisch den untergeordneten CAs.

Der Zertifikatsdienst von Windows 2000 hat die Aufgaben, Zertifikatsanforderungen zu akzeptieren, Zertifikate auszugeben und die Zertifikatsrückziehungsliste zu veröffentlichen. Zur Erstellung von Zertifikaten sind hier zahlreiche Vorlagen hinterlegt, die für verschiedene Zwecke vorgesehen

17 Eine der ersten Zertifizierungsstellen, sie bietet Client- und Server-Zertifikate

sind, es können jedoch auch eigene erstellt werden. Die gewünschten Vorlagen werden im Active Directory abgelegt und nur diese Zertifikate können dann ausgegeben werden.

Die Richtlinien für öffentliche Schlüssel werden in den Gruppenrichtlinien definiert. Hier kann beispielsweise vorgegeben werden, ob sich Benutzer Schlüssel von anderen als den eigenen CAs holen dürfen und ob sich Computer (nicht Benutzer!) selbst für Zertifikate registrieren können.

Fazit

Es gibt einige Applikationen in Windows 2000, die von der Einführung einer PKI profitieren können. Hierzu zählt der Webserver, da mit ihm dann vertrauenswürdige Kommunikation und auch E-Commerce für Clients möglich wird. Eine sichere E-Mail-Kommunikation kann mit Exchange durchgesetzt werden, da es Signaturen und Verschlüsselung unterstützt. Ein weiterer Vorteil ist die transparente Verwendung des Verschlüsselnden Dateisystems (EFS), bei dem die Daten im NTFS-Dateisystem verschlüsselt werden, diese für den Benutzer aber normal zu handhaben sind und nicht verschlüsselt erscheinen, für einen unbefugten Benutzer jedoch verschlüsselt sind.

2.1.8 IPSec

IPSec[18] ist eine Familie von Protokollen und kryptografischen Algorithmen, die das IP-Protokoll um Authentifizierung und Vertraulichkeit erweitert, um sichere Kommunikation über ein unsicheres Medium zu ermöglichen. Hauptsächlich wird die IP-Datagrammstruktur erweitert, indem ihr Vorspanne hinzugefügt werden; dadurch wird der Schutz der Daten ermöglicht und die Vorgänge sind transparent für Protokolle höherer Ebene. Die Entwicklung ging mit der Entwicklung von IPv6 einher und wurde dann zu IPSec modifiziert, da IPv6 noch nicht akzeptiert wurde. Es ist folglich als Erweiterung von IPv4 einzusetzen, damit man nicht unbedingt auf IPv6 übergehen muss. IPSec basiert auf Standarddokumenten der IETF, dabei gilt das [RFC2411] als zentrale Beschreibung, dass als IP Security Document Roadmap bekannt ist.

Die Verschlüsselung mit IPSec findet auf einer hohen Schicht statt, Router übermitteln nur die verschlüsselten Pakete, brauchen deshalb das IPSec-Protokoll nicht zu beherrschen und können die Pakete auch nicht selbst entschlüsseln, deshalb sind auch gesniffte (aufgezeichnete) Pakete verschlüsselt.

IPSec arbeitet auf der Netzwerkebene des OSI-Referenzmodells (Schicht 3), das bedeutet unter anderem, dass die gesamte ausgehende Kommunikation unabhängig von der Anwendung verschlüsselt wird. Im Gegensatz dazu ist es bei Verschlüsselungsprotokollen höherer Ebene, beispielsweise SSL, nötig, die Anwendungen anzupassen. Die Anpassung von Anwendungen entfällt hier vollkommen, da die komplette Palette der IP-Datagramme (TCP, UDP[19], ICMP[20], etc.) unterstützt und mitverschlüsselt wird. Dies geschieht völlig transparent für den Benutzer.

18 Internet Protocol Security

19 User Datagram Protocol

20 Internet Control Message Protocol

Unterstützte Sicherheitsfunktionen

IPSec beinhaltet einige Funktionen um die Sicherheit zu erhöhen, die man unterschiedlich miteinander kombinieren kann, je nachdem, wie sicher und performant die Übertragung geschehen soll.

Die *Authentifizierung* ermöglicht die eindeutige Identifikation des Senders und dieser kann im Nachhinein nicht abstreiten, die Information gesendet zu haben (non-repudiation). Außerdem kann die Identität eines Kommunikationspartners vor der Kommunikation überprüft werden. Ermöglicht wird dies in Windows 2000 über vor-veröffentlichte Public-Key-Verfahren oder Kerberos und Active Directory.

Für die *Verschlüsselung* wird DES oder 3DES[21] verwendet. Diese sind symmetrische Algorithmen, was bedeutet, dass beide Parteien Ver- und Entschlüsselungsschlüssel besitzen. Es werden 64 Bit große verschlüsselte Blöcke verwendet.

Vertraulichkeit wird durch eine Verschlüsselung der Daten erreicht, die nur für den Empfänger entschlüsselbar ist. Die eindeutige Identifikation des Senders, die durch eine Kombination aus Authentifizierung und Integritätsüberprüfung besteht, stellt die Authentizität des Sender eindeutig fest und belegt die Sendung der Information.

Mit Hilfe der *Anti-replay* -Funktion wird durch die Einmaligkeit der Pakete sichergestellt, dass Pakete nicht abgefangen und zu einem späteren Zeitpunkt noch einmal gesendet werden können. Dies könnte man beispielsweise mit einer abgefangenen Banküberweisung machen, die man einfach noch ein paar Mal sendet und die Überweisung dadurch mehrmals auslöst. Durch Sequenznummern, die Verwendung von CBC (Cipher Block Chaining) in Verbindung mit DES oder 3DES und einem Initalisierungsvektor (IV) wird erreicht, dass jedes Paket anders aussieht, selbst wenn es die gleichen Daten enthält. Damit wird es Angreifern erschwert, Informationen aus abgefangenen Paketen weiterzuverwenden, um sie beispielsweise später selber zur Anmeldung zu benutzen, den Datenverkehr zu analysieren und den Inhalt der Pakete lesen zu können.

Die *Integrität* und somit die Unversehrtheit der Daten wird durch Signierung über kryptografische Hashfunktionen mit Hilfe von HMACs (Hash Message Authentication Codes) sichergestellt, beispielsweise werden die Pakete mit MD 5 (Message Digest 5) signiert, was als verschlüsselte Prüfsumme oder MIC (Message Integrity Code) bekannt ist. Diese Information wird angefügt und beim Empfang wieder berechnet. Bei Änderungen des Inhalts stimmen die Signaturen nicht miteinander überein und das Paket wird sofort gelöscht. Nur bei Übereinstimmung der Signaturen wird das Paket weitergereicht.

Außerdem ist eine *Schlüsselverwaltung* integriert, die die Unterstützung für die Schlüsselgenerierung, den Schlüsselaustausch und die Schlüsselaktualisierung übernimmt.

---

21 3DES ist eine Variante mit 3facher Verschlüsselung

Verschlüsselung

IPSec verwendet zwei Protokolle für zwei verschiedene Sicherheitsstufen: AH *(IP Authentication Header)* und ESP *(IP Encapsulating Security Payload)*. Diese können getrennt oder auch in Kombination verwendet werden.

Authentication Header stellt Authentifizierung, Anti-replay und Integrität für das gesamte Paket sicher, verschlüsselt dieses aber nicht. Somit können Sender, Empfänger und die Unversehrtheit der Daten sichergestellt, nicht aber deren Abfangen verhindert werden. Es wird als AH-Header hinter den IP-Header angehängt und somit im Paket übertragen.

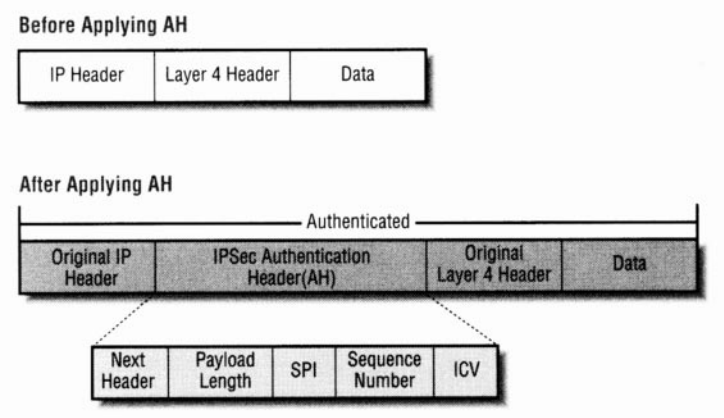

Abbildung 2-13 „An IPSec datagram with Authentication Header" [NOR01]

Encapsulating Security Payload bietet Verschlüsselung, Authentifizierung, Anti-replay und Intergrität und kapselt im Gegensatz zu Authentication Header die Daten in seiner Protokollstruktur. Nur der IP-Header, der bei AH signiert ist, ist nicht signiert und deshalb kann ein Angreifer den IP-Header verändern, ohne dass der Empfänger es bemerkt. Um hierfür einen Schutz zu erreichen, kann man allerdings AH mit ESP kombinieren.

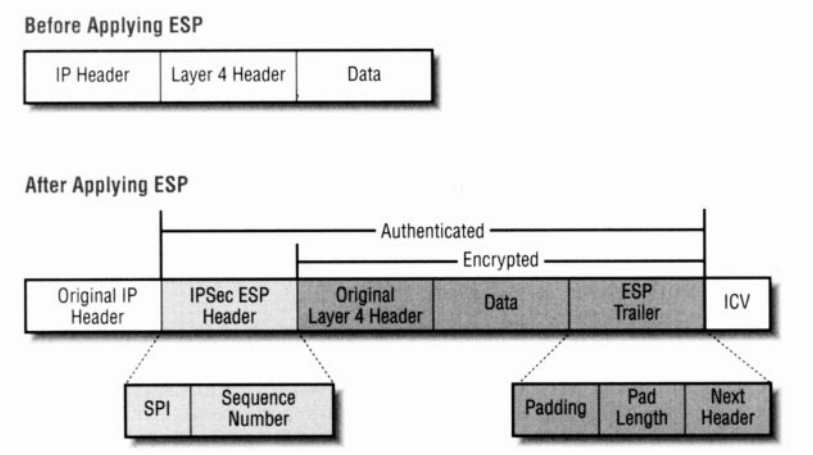

Abbildung 2-14 „An IPSec datagram with Encapsulating Security Payload" [NOR01]

Es existieren verschiedene Transportmodi. Beim normalen *Transportmodus* müssen nur die Endsysteme IPSec unterstützen, die weiterleitenden (Router, etc.) jedoch nicht. Er läuft auf höherer Schicht ab und ist für End-zu-End-Übertragung geeignet. Es wird ein zusätzlicher Vorspann zwischen IP-Datagramm und den Daten eingefügt. Der Transportmodus ist für geringe Sicherheit ausreichend.

Für maximale Sicherheit gibt es den *Tunnelmodus,* der zwei Gateways miteinander verknüpft. Er ist für Router geeignet, um auf einer unsicheren Verbindung sichere Übertragung zu ermöglichen. Dabei wird das IP-Datagramm in ein anderes IP-Datagramm gepackt (getunnelt) und somit ist das Original-IP-Datagramm vollständig verschlüsselt. Hierbei wird das gesamte IP-Paket vom Sender gekapselt, indem er einen völlig neuen Vorspann generiert. Mit Hilfe von ESP wird es verschlüsselt und mit AH signiert und enthält somit den alten und den neuen Vorspann. Das Resultat ist ein sicherer Tunnel in einem unsicheren Netzwerk. Dabei müssen nicht einmal die Endsysteme IPSec oder überhaupt TCP/IP beherrschen, sondern nur die Gateways, die den Tunnel herstellen. Hierbei kann man IPSec selbst oder L2TP verwenden, das eine Kombination aus PPTP (Point-To-Point Tunneling Protocol) und L2F (Layer 2 Forwarding von Cisco) zum Erstellen des Tunnels verwendet.

ESP-Tunnel arbeiten auf OSI-Schicht 3 und können nur IP-Pakete tunneln; da L2TP-Tunnel auf Schicht 2 arbeiten, können in ihnen auch z.B. IPX, NetBEUI, etc. getunnelt werden.

Funktionsweise

IPSec erstellt *IPSec-Sicherheitszuordnungen* (Security Association = SA) zwischen zwei Rechnern und transformiert mit diesen die IP-Datagramme, um diese zu schützen; dabei sind unterstützte Transformationen AH (Authentifizierungs-Header) und ESP (Encapsulating Security Payload). Diese Sicherheitszuordnungen werden vor dem IP-Paketaustausch ausgehandelt und enthalten Details wie die Schlüssel, deren Gültigkeit und Authentifizierungs- und Verschlüsselungsprotokolle, wobei die Systemrichtlinien die aushandelbaren Optionen festlegen.

Zur Benutzung von IPSec werden zwei Sicherheitszuordnungen erstellt.

1. Die *ISAKMP-SA* (Internet Security Association and Key Management Protocol), die die Systemrichtlinienauswahl, das Anlegen der ISAKMP-SA, den Schlüsselaustausch und die Computerauthentifizierung beinhaltet. Außerdem wird hiermit die Möglichkeit zur Bildung weiterer SAs gelegt.
2. Mit der ISAKMP-SA werden die IPSec- Sicherheitszuordnungen ausgehandelt, die die Transformation der Daten erledigen.

Der *Sicherheitsparameterindex* (SPI) wird in den AH- oder ESP-Vorspannen der IP-Datagramme übermittelt und ist eine 32-Bit-Zufallszahl, die zur Identifikation der IP-Pakete für die SA benötigt wird.

Zur Verwaltung dienen *IPSec-Systemrichtlinien*; in ihnen werden die zuzulassenden Kommunikationsarten ausgewählt und entschieden, wie diese geschützt werden sollen. Dann werden diesen Benutzer und Gruppen oder andere Active Directory Objekte zugeordnet. Die *IPSec-Systemrichtlinien* beschreiben das Verhalten der Computer beim Datenaustausch über IPSec und enthalten folgende Regeln:

- *Filter-Liste* enthält zu sichernden Verkehr
- *Filter-Aktionen* geben Vorgehen mit Verkehr, der der Filter-Liste entspricht, vor
- *Authentifizierungsmethoden* wie Kerberos, Public Key oder X509
- *Verbindungstypen* wie LAN, WAN oder beides
- *Tunneleinstellungen*, die Angabe von Tunnelendpunkten für IPSec-Tunnel enthalten

Hinzu kommen noch einige Echtzeitkomponenten:

Der *IPSec-Richtliniendienst-Agent* arbeitet auf jedem IPSec unterstützenden System, fragt die Systemrichtlinien beim Active Directory oder der lokalen Registrierung ab und liefert sie an andere IPSec-Komponenten, etwa den IPSec-Treiber, weiter.

Der *Internetschlüsselaustausch* (Internet Key Exchange - IKE), der ein Protokoll zum Erstellen einer Sicherheitszuordnung und den Schlüsselaustausch darstellt, umfasst zwei Phasen in denen eine authentifizierte Kommunikation aufgebaut und die Art der IPSec Kommunikation ausgewählt wird.

Der *IPSec-Treiber* enthält die IP-Filterliste. Wenn ein ausgehendes Paket registriert wird, lässt er den IKE den Schlüsselaustausch mit dem Zielsystem beginnen und verschlüsselt dann die Pakete. Bei eingehenden Paketen wird die Signatur überprüft und dann werden die Pakete bei Übereinstimmung entschlüsselt und ansonsten gelöscht.

Es ist möglich, die Verschlüsselung nach einer bestimmten Zeit oder einem bestimmten Datenvolumen automatisch ändern zu lassen, um die Sicherheit zu erhöhen. Dies wird ebenfalls in den Richtlinien festgelegt.

Konsequenzen und Probleme

IPSec belastet das Netzwerk durch den IKE-Verkehr und die veränderten Header. Außerdem erhöht sich die Prozessorauslastung durch die Ver- und Entschlüsselung und durch Integritätsberechnungen. Bei der höchsten Sicherheitseinstellung könnte man eventuell deutliche Performanceeinbußen messen.

IPSec steht momentan nur für Windows 2000 zur Verfügung. Plattfomen wie Windows 95, 98,NT oder Unix und Apple Macintosh werden nicht unterstützt.

Virtuelle Private Netzwerke

Es ist möglich, Virtuelle Private Netzwerke (VPN – Virtual Private Network) mit Rechnern mit installiertem Windows 2000 aufzubauen. Dafür wurde das Protokoll PPTP (Point-to-Point Tunneling Protocol) entwickelt, Windows 2000 beherrscht allerdings auch das L2TP (Layer 2 Tunneling Protocol), das von der IETF als offener Standard definiert wurde. Dieses ist eine Kombination aus PPTP und L2F(Layer 2 Forwarding) von Cisco Systems. Beide Protokolle sind reine Tunnelprotokolle, arbeiten auf OSI-Schicht 2 und setzen die Pakete in andere Pakete, Adressen und Protokolle um, verschlüsseln sie jedoch nicht [HAR99].

Fazit

IPSec verhindert das Lesen der Pakete, das Ausspionieren von Schlüsseln und Passwörtern, die Verwendung einer falschen Identität und die Veränderung der Daten, jedoch nicht das Abfangen der Pakete durch Sniffing. Außerdem ermöglicht es das Filtern von Paketen, um den Netzwerkverkehr auf Basis von IP-Adressen, Protokollen und Ports zu regeln. Somit ist eine Möglichkeit gegeben, um Denial-Of-Service-Angriffe bis zu einem gewissen Grad zu verhindern, indem Pakete von nicht vertrauenswürdigen Adressen verworfen werden. Dies stellt eine einfache Art einer Firewall dar.

2.1.9 Secure Sockets Layer (SSL) und Transport Layer Security (TLS)

Die Übertragung von Daten in unsicheren Netzwerken und die sichere *Authentifizierung* von Benutzern kann durch verschiedene Protokolle auf unterschiedlichen Ebenen erfolgen. Während *IPSec* meist auf der Protokollebene des *OSI-Modells* arbeitet, werden das *Secure Sockets Layer-(SSL)* und das *Transport Layer Security*-Protokoll (TLS) direkt in den Anwendungen implementiert und unterstützen ein anderes Protokoll (z.B. HTTP) bei der Übertragung von sensiblen Daten. Beide Protokolle bieten eine Benutzerauthentifizierung, sowie Vertraulichkeit und Integrität der übertragenen Daten.

Zertifikate

Ein *Zertifikat* ist eine Sammlung von Informationen. Dazu gehört z.B. der Name, die Adresse und andere Information des Zertifikatseigners. Der Eigentümer besitzt ein *kryptographisches Schlüsselpaar*, das aus einem öffentlichen und einem privaten Schlüssel besteht. Während der private Schlüssel nur vom Eigentümer besessen werden darf, wird der öffentliche Schlüssel Teil des Zertifikats. Das komplette Zertifikat bekommt ein Gültigkeitsdatum und wird dann von einer *Zertifizierungsstelle* signiert, deren Adresse ebenfalls Bestandteil des Zertifikats ist.
Die *Signierung* eines Zertifikats durch eine Zertifizierungsstelle wird mit Hilfe des Zertifikats der Zertifizierungsstelle überprüft. Durch diese Verkettung von Zertifizierungsstellen und Zertifikaten entsteht eine *Vertrauenshierarchie*.

Zertifizierungsstellen

Durch die Signierung eines Zertifikats durch eine Zertifizierungsstelle, vertraut ein Benutzer dem Zertifikat, wenn er auch der Zertifizierungsstelle vertraut, und eine Zertifizierungsstelle kann mit dieser Technik beliebig viele Zertifikate ausstellen. Die Zertifikate der vertrauenswürdigen Zertifizierungsstellen werden in der *Zertifikatsvertrauensliste (CTL)* gespeichert. Die Signatur eines un-

bekannten Zertifikats kann dann mit Hilfe der öffentlichen Schlüssel der Zertifizierungsstellen, die in der CTL gespeichert sind, überprüft werden.

1. Verlangt der Server eine Authentifizierung des Client, sendet er eine Anforderung an den Client. Dieser signiert die Anforderung mit dem privaten Schlüssel seines Clientzertifikats und sendet die signierte Anforderung mit seinem Clientzertifikat und seinem öffentlichen Schlüssel an den Server.
2. Der Server kann nun die Echtheit des Zertifikats überprüfen und mit dem öffentlichen Schlüssel des Clients die Signatur der Anforderung testen. Ist diese in Ordnung und vertraut der Server dem Clientzertifikat, gilt der Client als authentifiziert.

Entscheidend für die sichere Übertragung ist nun die Länge des symmetrischen Sitzungsschlüssels. Diese Länge kann 40,56 oder 128 Bit betragen, wobei eine 128 Bit Verschlüsselung als sicher gilt. Windows 2000 unterstützt alle Schlüssellängen, wenn das *High Encryption Pack* oder Service Pack 2 installiert ist. Microsoft hat die Genehmigung für den Export der 128 Bit Verschlüsselung bekommen, wobei neun Staaten ausgenommen sind, für die ein US-Embargo gilt.

Transport Layer Security (TLS)

Das *Transport Layer Security-Protokoll* basiert auf das SSL 3.0-Protokoll von Netscape, ist aber nicht direkt mit SSL kompatibel. Aus diesem Grund bietet das Protokoll Methoden, sich wie ein SSL Protokoll zu verhalten, um eine Abwärtskompatibilität zu gewährleisten. Das TLS-Protokoll wird in [RFC2246] als Version 1.0 definiert. Es bietet dabei folgende Leistungsmerkmale:

- **Sichere Verbindung zwischen zwei Partnern**
  Die Übertragung der Daten erfolgt in verschlüsselter Form, so dass ein Dritter zwar die Daten abfangen kann, aber nur den verschlüsselten Datenstrom erhält. Neben der Vertraulichkeit der Daten wird die Identität der Partner gewährleistet. So kann sich kein Dritter als einer der beiden Partner ausgeben.
- **Sichere Implementierung**
  Es soll gewährleistet sein, dass unterschiedliche Entwickler dieses Protokoll unabhängig voneinander in ihre Anwendungen implementieren und diese Programme einwandfrei miteinander kommunizieren können. Dazu muss das Protokoll natürlich auch unabhängig von der verwendeten Plattform sein.
- **Erweiterbarkeit**
  Das Protokoll soll in der Zukunft erweitert werden können. Dazu müssen die jetzt entstehenden Implementierungen in der Lage sein, neue Protokollversionen zu verarbeiten und neue Protokollversionen müssen abwärtskompatibel sein.
- **Effektivität**
  Da Verschlüsselungsmethoden immer zu Lasten der Performance gehen, soll das Protokoll möglichst effizient sein, um das System nicht unnötig zu belasten.

Das Protokoll besteht aus zwei Schichten: dem *TLS-Record Protokoll* und dem *TLS Handshake-Protokoll*. Beide liegen oberhalb der Transportschicht, wobei das TLS-Record Protokoll unterhalb des TLSHandshake-Protokolls angeordnet ist.

Das TLS Handshake-Protokoll ist für die Authentifizierung der Kommunkationspartner zuständig. Dies geschieht über *Public Key Verfahren* und sollte zumindest einen Partner authentifizieren. Außerdem erzeugt das TLS-Handshake Protokoll den gemeinsamen Sitzungsschlüssel, der für die Verschlüsselung des Datenstroms verwendet wird *(TLS master secret)* und handelt die verwendeten Verschlüsselungsmethoden aus.
Eine TLS-Sitzung findet über die gleichen Verbindungsports statt, wie das ebenso verwendete SSL-Protokoll. So erwartet ein HTTP-Server eine Anforderung für eine sichere Verbindung immer am gleichen TCP-Port, unabhängig vom verwendeten Verschlüsselungsprotokoll. TLS-Client- und Serverprotokolle müssen daher auch mit SSL Verbindungsanforderungen umgehen können und diese entsprechend behandeln.
Das TLS-Record Protokoll übernimmt die zu übermittelnden Daten, zerteilt sie in kleinere Pakete, komprimiert die Daten, versieht sie mit einer Seriennummer, verschlüsselt die Daten und versendet diese. Empfangene Daten werden entschlüsselt, überprüft, dekomprimiert, zusammengefügt und an die höhere Netzwerkschicht übermittelt. Es sind noch weitere Protokolle vorhanden, die in TLS definiert sind:

- **Alert Protokoll**
  Beide Partner können eine Warnung oder Fehlermeldung in komprimierter Form an den anderen Partner senden. Sollte es sich um einen schwerwiegenden Fehler handeln, der evtl. auf einen Angreifer schließen lässt, wird die Verbindung abgebrochen und alle vereinbarten Schlüssel gelöscht.
- **Change Cipher Spec Protokoll**
  Dieses Protokoll verwendet eine Nachricht, um dem Record Layer die Verwendung von neuen Keys oder Verschlüsselungsmethoden mitzuteilen. Die Nachricht wird mit der bisherigen Verschlüsselungsmethode verschlüsselt.
- **Application Data Protokoll.**
  Dieses Protokoll ist für die eigentliche Datenübermittlung verantwortlich.

Anforderung von Zertifikaten

Damit SSL bzw. TLS mit einem Server verwendet werden kann, benötigt dieser ein kryptographisches Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel und ein von einer Zertifizierungsstelle signiertes Zertifikat. Um solch ein Zertifikat zu erhalten, wird eine Zertifikatsanforderung erstellt, die alle notwendigen Daten, wie Name, Adresse des Eigentümers, bei einem Webserver die Domäne der Website und weitere Daten enthält. Zusammen mit dem öffentlichen Schlüssel des Servers wird diese Anfrage an eine Zertifizierungsstelle geschickt, die allgemeines Vertrauen genießt. Dies ist wichtig, da das Vertrauen an das Zertifikat vom Vertrauen an die Zertifizierungsstelle abhängig ist.
Soll die Verschlüsselung nur innerhalb eines Intranets verwendet werden, kann natürlich auch eine eigene Zertifizierungsstelle eingerichtet werden, die dann kein Vertrauen außerhalb des Unternehmens genießt, intern aber vertrauenswürdig ist.
Die Zertifizierungsstelle muss nun die Anfrage überprüfen und die Identität des Anfragenden sicherstellen. Dies muss von der Zertifizierungsstelle gewissenhaft erledigt werden, da die eigene Vertrauenswürdigkeit davon abhängt.

Danach wird die Zertifizierungsstelle das angeforderte Zertifikat erstellen und es mit ihrem privaten Schlüssel signieren. Eine Änderung des Zertifikats ist danach nicht mehr möglich, ohne die Signatur zu erneuern. Das Zertifikat kann dann von der Zertifizierungsstelle abgeholt und verwendet werden.

Verwendung von SSL/TLS

Ist ein Schlüsselpaar erzeugt und ein Zertifikat erstellt, kann es für die Verwendung von SSL/TLS verwendet werden. Die genaue Vorgehensweise hängt dabei von dem verwendeten Server ab. Dies soll am Beispiel eines Webserver verdeutlicht werden.
Die Aktivierung eines SSL geschützten Webservers beginnt bei der Erstellung einer Zertifikatsanfrage für eine bestimmte Domäne. Jede Domäne benötigt ein eigenes Zertifikat, da sie Bestandteil der Information ist, die auf dem Zertifikat festgehalten ist.
Nachdem das fertige Zertifikat von der Zertifizierungsstelle erhalten wurde, wird es im Webserver installiert und die SSL Verschlüsselung aktiviert.
Natürlich können auch andere Verbindungen mit SSL/TLS verschlüsselt werden. Windows 2000 bietet für eine ganze Reihe von Diensten eine SSL-Verschlüsselung an. Dazu gehören SMTP, POP3 und NNTP, wobei die Einrichtung ähnlich abläuft.

Zusammenfassung

SSL und TLS sind zwei Protokolle, mit denen sich Übertragungen über Netzwerke sichern lassen. Sie sorgen für Integrität und Vertraulichkeit der Daten und können zur Authentifizierung von Verbindungspartnern verwendet werden. Die häufigste Verwendung findet zur Zeit für die sichere Übertragung von Internetseiten statt. Beide Protokolle basieren auf eine symmetrische Verschlüsselung der Daten, den Austausch von öffentlichen Schlüsseln und die Verwendung von Zertifikaten, die durch Zertifizierungsstellen erstellt und signiert werden und die untereinander eine Vertrauenshierarchie aufbauen.

2.2 Integrierte Komponenten von Windows 2000

Die Windows 2000 Server Version enthält bereits in der Standardinstallation eine Vielzahl von Diensten und Anwendungen, die es zu kennen und zu konfigurieren gilt. Aber auch die Clientversion erlaubt die Installation dieser Komponenten und ein experimentierfreudiger Anwender mag dazu ermutigt werden.
Obwohl das Betriebssystem viele dieser Anwendungen benötigt, um ein Windows 2000 Netzwerk aus Server und Clients zu betreiben, sind einige Komponenten optional und können bei falscher Konfiguration zu großen Sicherheitsproblemen führen. Dieses Kapitel gibt einen Einblick in die Windows 2000 Komponenten und erklärt ihre Funktionen.

2.2.1 Component Object Model (COM, DCOM) und COM+

Das *Component Object Model (COM)* spielt eine zentrale Rolle in der Systemarchitektur, war allerdings in der Vergangenheit nur für Anwendungsentwickler von wirklichem Interesse, da die Funktionalität von COM sich meist im Hintergrund abspielte.

Mit der Einführung von *COM+* kommen nun plötzlich auch Administratoren mit der COM Architektur in Kontakt und sind in der Lage, Einstellungen mit nur einem Mausklick zu verändern. Aus diesem Grund ist es mehr und mehr erforderlich zu wissen, was sich hinter den Komponenten verbirgt.

Was ist COM?

Das Component Object Model ist zunächst eine Beschreibung von Schnittstellen, die bspw. ein Programmierer verwenden kann. Ein Entwickler hat ein Programm geschrieben, dass in der Lage ist E-Mails zu versenden und er möchte anderen Entwicklern diese Funktion ebenfalls zur Verfügung stellen. Während der Benutzer eine E-Mail durch Interaktion mit einer Anwendung verschickt, benötigt ein Entwickler eine Methode, um das E-Mail-Programm direkt anzusteuern. Besitzt das Programm eine *COM-Schnittstelle*, kann der Entwickler diese verwenden, um mit dem E-Mail-Programm eine E-Mail zu versenden. Was so einfach klingt, gestaltet sich aus Sicht eines Entwicklers schwierig, da ein Programm in unterschiedlichen Programmiersprachen geschrieben sein kann oder sich auf einem anderen Computer befinden könnte.
Das Component Object Model beschreibt nun eine binäre Schnittstelle, die von unterschiedlichen Programmier- und Scriptsprachen verwendet werden kann. Wenn Entwickler A eine Programmiersprache verwendet, die COM unterstützt und Entwickler B seinem Programm eine COM-Schnittstelle hinzufügt, dann kann A die Funktionen des Programms von B nutzen, die in der COM Schnittstelle zur Verfügung gestellt wurden.
Komponenten mit einer COM-Schnittstelle können allerdings auch vorhandene Programme in der Funktionalität erweitern. Ein Bildverarbeitungsprogramm kann z.B. Programmerweiterungen zulassen, die ein Bild manipulieren. Die einzelnen Erweiterungen können COM-Objekte sein, die eine Reihe von Funktionen unterstützen müssen. Das Bildprogramm übergibt das Bild an die Komponente und erhält das veränderte Bild als Ergebnis. Der Entwickler, der das Bildprogramm geschrieben hat, muss nicht wissen, mit welcher Programmiersprache die zusätzlichen Filter entwickelt worden sind, er muss lediglich die verwendeten Funktionen vorgeben. Ein anderer Entwickler kann dann seine favorisierte Programmiersprache verwenden und zusätzliche Module entwickeln. Solche Techniken werden in Windows 2000 ständig eingesetzt. Kaum ein Programm oder Dienst kommt ohne COM aus. Ein Webserver, der Daten von einer Datenbank abfragt, verwendet COM für die Abfrage genauso, wie eine Textverarbeitung, die gerade Briefe ausdruckt. Mit Hilfe von COM können Anwendungen oder Prozesse in kleinere Module zerlegt werden, die eine effektivere Entwicklung ermöglichen.
Da solche Aufrufe auch über Rechnergrenzen hinweg geschehen können, ist es wichtig, die Sicherheitsfunktionen zu kennen.

Entwicklung von COM

Die Open Software Foundation entwickelte gegen Ende der 70er Jahre den *Remote Procedure Call (RPC)*-Standard, um eine Schnittstelle zwischen verschiedenen Programmen zu schaffen. Diese verwendete allerdings keine *objektorientierte Programmierung (OOP)*, die immer beliebter wurde. Microsoft setzt daher seit Ende der 80er Jahre die objektorientierte COM-Technologie für Windows NT ein.

Schnittstellen

COM-Objekte können von unterschiedlichen Firmen und Entwicklern erstellt werden. Damit diese Objekte eindeutig sind, erhalten sie eine 128 Bit lange Nummer, die GUID genannt wird und während der Entwicklung eines COM-Objekts erstellt wird. Sie entsteht aus dem Datum und der Uhrzeit, der Hardwareadresse einer evtl. vorhandenen Netzwerkkarte und anderen Informationen, die eine weltweite Eindeutigkeit garantieren sollen. Zusätzlich kann noch ein Name vergeben werden, der dann durch die Verwendung von Firmen- oder Produktnamen, eindeutig gemacht wird.
Ein Programm kann über diese Nummern oder den Namen eine Instanz des COM-Objekts erzeugen und diese verwenden. Welche Methoden das Objekt versteht, wird durch Schnittstellen beschrieben, deren Format durch COM definiert ist.
Eine Komponente kann dabei mehrere Schnittstellen besitzen, es hat aber immer eine *Standardschnittstelle* (mit dem Namen *‚IUnknown'*), die Methoden bereitstellt um Informationen über die Komponente zu erhalten. Die Schnittstellen werden in einer Tabelle gespeichert und können über Methoden, die durch COM beschrieben werden, ausgelesen werden.
Die Standardschnittstelle enthält außerdem einen Referenzzähler, der um eins erhöht bzw. verringert wird, wenn eine Objektinstanz erzeugt bzw. zerstört wird. Dadurch kann jederzeit festgestellt werden, ob ein Objekt noch in Verwendung ist, damit es z.B. nicht versehentlich aus dem Dateisystem entfernt wird. Erst wenn der Referenzzähler Null ist, wird die Komponente freigegeben.

DCOM

Im Component Objekt Model fehlte eine entscheidende Funktion, die nachträglich hinzugefügt wurde. Die COM-Schnittstellen ermöglichten nicht die Verwendung von Funktionen über Rechnergrenzen hinweg, z.B. über ein Netzwerk. Diese *Distributed COM (DCOM)*-Definition ergänzte das Component Object Model um diese fehlenden Funktionen. Dabei wurde wieder RPC als Transportmechanismus eingesetzt, so dass es möglich wurde, eine Komponente auf einem anderen Rechner über ein Netzwerk zu verwenden.

COM+

Die *COM+-Technologie*, die in Windows 2000 zum Einsatz kommt, ist eine Erweiterung der COM-Spezifikationen, um weitere Dienste und Funktionen. Der Microsoft Transaction Server, der Transaktionen[22] ermöglicht, wurde in Windows 2000 zum *Microsoft Komponentendienst* und erlaubt die Einrichtung und Verwaltung von COM+-Komponenten. Der Komponentendienst hat seinen Platz in der Windows-Verwaltung gefunden. Eine COM+-Komponente bietet nun weitere Funktionen auf der Basis einer COM-Komponente:

- **Transaktionsverwaltung**
  Die Integration des Transaction Servers in die Komponentendienste hat die Aufgabe, die COM+-Komponenten transaktionsfähig zu machen. Dafür müssen die COM-Objekte diese Funktionalität ermöglichen.

22 Eine Transaktion ist eine Folge von Aktionen. Wird eine Aktion abgebrochen oder mit einem Fehler beendet, werden alle vorherigen Aktionen wieder rückgängig gemacht.

- **Komponenten-Lastausgleich (CLB, Component Load Balancing)**
  Identische COM+-Objekte auf mehreren Servern werden miteinander verknüpft, so dass Aufrufe für dieses COM+-Objekt auf mehrere Server verteilt werden können.
- **Warteschlangen**
  Verwendet ein Programm die Funktionalität einer Komponente, so geschieht dies normalerweise synchron, d.h. das Programm ruft die Funktion auf und wartet auf das Ergebnis. Mit COM+ können diese Aufrufe nun asynchron erfolgen, d.h. ein Programm ruft Funktionen einer Komponente auf, die jedoch in einer Warteschlange abgelegt werden. Während das Programm sich nicht mehr um die Aufrufe kümmern muss, sorgt die Warteschlangenfunktion in COM+ für dessen Ausführung. Ein Beispiel für solch ein Aufruf, wäre das Versenden einer E-Mail. Das Client-Programm ruft eine Komponente auf und übergibt die E-Mail. Die Komponente versendet diese dann, wenn z.B. eine Internetverbindung hergestellt oder der Mailserver erreichbar wird.
- **Object Pooling**
  Wird eine Instanz von einem COM-Objekt erzeugt, so wird diese in den Speicher geladen, um Aufrufe zu ermöglichen. Normalerweise wird die Instanz nach der Zerstörung wieder aus dem Speicher entfernt. Beim Object-Pooling verbleibt diese Instanz nun im Speicher und kann wieder verwendet werden, wenn eine neue Instanz erstellt wird. Da das Erzeugen einer neuen Instanz etwas Zeit benötigt, kann diese Funktion den Ablauf beschleunigen, wenn z.B. eine Webanwendung für jeden neuen Besucher eine Instanz erzeugt und diese wieder vernichtet, sobald der Besucher verschwunden ist.
- **Speicherresistente Datenbanken**
  Diese Datenbanken, die im RAM gespeichert werden, sind extrem schnell und können von COM+-Komponenten verwendet werden, wenn Prozesse sehr schnell ablaufen müssen.
- **Sicherheitsfunktionen**
  Eine der wichtigsten Funktionen ist die Sicherheitsverwaltung der COM+-Komponenten. Es können unterschiedliche Sicherheitsfunktionen genutzt werden, die von den Komponentendiensten bereitgestellt werden.

Zusammenfassung

Das COM-Modell definiert Schnittstellen für objektorientierte Komponenten. Diese sind unabhängig von der verwendeten Programmiersprache und arbeiten auf binärer Ebene.
COM-Komponenten können dazu verwendet werden, Programme in einzelne Module zu unterteilen. Durch die Erweiterung durch COM+ und die Verwendung von COM-Objekten z.B. in Websites, werden die Konfigurationen von COM+-Anwendungen mehr und mehr zur Sache eines Windows-Administrators, so dass sich dieser auch damit auseinandersetzen muss.

2.2.2 Dynamic Host Configuration Protocol (DHCP)

Damit ein Computer in einem TCP/IP Netzwerk kommunizieren kann, müssen eine Reihe von Einstellungen am Computer vorgenommen werden. Der Computer benötigt eine im Netzwerk eindeutige IP-Adresse, eine Netzwerkmaske und evtl. andere Daten, wie eine *DNS-Server*- oder eine *Gateway-Adresse*.

Die richtige Konfiguration einer Vielzahl von Computern im Netzwerk kann zu einem größeren Verwaltungsaufwand werden und eine Änderung an der Netzwerkstruktur kann Änderungen an den Konfigurationen der Computer im Netzwerk bedeuten.
Das *Dynamic Host Configuration Protocol (DHCP)* vereinfacht diese Aufgaben. Das Client/Server basierte Protokoll vergibt Adressen und Netzwerkeinstellungen an Clientcomputer über einen zentralen Server. Ist dieser richtig konfiguriert, beziehen die Clients alle notwendigen Informationen von ihm und die Administration der Netzwerkadressen und -daten erfolgt zentral dort.
Die IETF definiert das DHCP-Protokoll in den [RFC2131] und [RFC2132] und es wurde auf Grundlage des BOOTP-Protokolls entwickelt.

DHCP Client und Server

Das DHCP-Protokoll defniert DHCP-Clients als Computer, die Einstellungsdaten von einem *DHCP-Server* beziehen und setzt das Vorhandensein eines DHCP-Server eigentlich voraus. *DHCP-Clients* sind allerdings auch ohne DHCP-Server in der Lage, eine Adresse zu finden und können dann untereinander kommunizieren.

Geltungsbereiche und Optionen

Ein DHCP-Server besitzt mindestens einen Pool von zusammenhängenden IP-Adressen, die er an Clients vergeben kann. Solch ein zusammenhängender Bereich von IP-Adressen wird *DHCP-Geltungsbereich* genannt. Dabei überprüft der DHCP-Server jedoch nicht, ob die Adressen schon von anderen Computern verwendet werden, sondern geht davon aus, dass er für die Vergabe der Adressen aus dem Geltungsbereich allein verantwortlich ist. DHCP-Server dürfen also keine Überschneidungen in den Geltungsbereichen haben, da sich diese Server auch nicht untereinander abgleichen. Manuell konfigurierte Computer dürfen keine Adressen aus vorhandenen DHCP-Geltungsbereichen verwenden.
Innerhalb eines Geltungsbereichs kann der DHCP-Server weitere Einstellungen an die Clients übermitteln, die DHCP-Optionen genannt werden. Weitere Informationen können z.B. die Adresse des Nameservers oder der verwendete Domänenname sein. Bei Einsatz eines DHCP-Servers unter Windows 2000 werden die Optionen in fünf Ebenen verwaltet:

- **Vordefinierte Optionen**
  Diese legen Standardwerte für Optionen fest.
- **Serveroptionen**
  Diese Optionen gelten für alle Geltungsbereiche und Clients, die auf dem DHCP-Server definiert sind.
- **Geltungsbereichsoptionen**
  Diese gelten nur für Clients, die in dem Geltungsbereich definiert sind. Die Geltungsbereichsoptionen können Werte der Serveroptionen überschreiben.
- **Klassenoptionen**
  Klassen können benutzer- oder herstellerspezifisch sein. Es können bestimmte Benutzer mit anderen Informationen versorgt werden oder Klassen für bestimmte Betriebssysteme (z.B. Windows 2000) definiert werden. Diese Optionen werden nur durch Optionen auf der Clientebene überschrieben. Für ältere DHCP-Clients, die keine Klasseninformationen an den Server senden, kann eine Standardklassen definiert werden.

- **Clientoptionen**
  Diese Optionen, die für einzelne DHCP-Clients explizit angegeben werden können nur noch durch manuell eingestellte Eigenschaften auf dem Clientcomputer überschrieben werden.

DHCP-Lease

Die erhaltenen IP-Adressen werden nur für einen gewissen Zeitraum vergeben und sind vom Server lediglich "gemietet" *(DHCP-Lease)*. Die Dauer einer solchen Lease ist im DHCP-Server einstellbar. Da nach Ablauf der Lease der Client die IP-Adresse wieder verlieren würde, versucht er nach der Hälfte der Zeit seine Lease zu erneuern. Wenn der erste Versuch misslingt, wird nach 3/4 der Zeit ein neuer Versuch unternommen. Sollte die Aktualisierung der Lease nicht funktionieren, muss der Client die IP-Adresse nach Ablauf der Lease freigeben.
Der DHCP-Server verwaltet eine Tabelle, in der festgehalten wird, welche IP-Adresse eine Netzwerkkarte zuletzt erhalten hat und er wird bei einer Anfrage versuchen, diese erneut zu verwenden, solange sie nicht schon wieder vergeben wurde. In Windows 2000 hat der Administrator die Möglichkeit diese Tabelle selbst zu erweitern, um spezielle Clients mit entsprechenden MAC-Adressen bestimmte IP-Adressen zuzuordnen.

DHCP-Nachrichten

Die zwischen dem Server und dem Client ausgetauschten Informationen werden *DHCP-Nachrichten* genannt. Die Übertragung der Daten zwischen Client und Server erfolgt dabei mit Hilfe von UDP (User Data Protocol). Verfügt der Client über eine gebundene IP-Adresse, kommunizieren Client und Server über Unicast-IP-Datagramme, während Clients, die sich im Prozess der Zuweisung einer IP-Adresse befinden, Broadcast-Pakete an die Adresse 255.255.255.255 senden. DHCP-Clients verwenden dabei den UDP-Port 68 und Server den UDP-Port 67. Die acht Nachrichtentypen lauten wie folgt:

- **DHCPDISCOVER**
  Ein Client verwendet diese Nachricht, um eine IP-Adresse von einem Server anzufordern. Dies ist der erste Schritt für den der Client noch keine eigene IP-Adresse besitzt. Daher wird diese Nachricht an die Broadcast Adresse 255.255.255.255 gesendet, als Quelladresse 0.0.0.0 verwendet und der Client identifiziert sich mit seiner MAC-Adresse. Windows 2000 Computer senden in dieser Nachricht zusätzliche Informationen, wie den Hostnamen und die Clientklasse.
- **DHCPOFFER**
  Die DHCPOFFER Nachricht wird von einem Server gesendet, um eine IP Adresse anzubieten. Auch diese Nachricht wird als UDP Multicast Paket an UDP Port 68 gesendet, da der Client noch keine IP-Adresse besitzt. In der Nachricht sind die angebotene IP-Adresse, die IP-Adresse des DHCP-Servers und die Hardwareadresse (MAC) des Clients, der eine DHCPDISCOVER Nachricht gesendet hat, enthalten.
- **DHCPREQUEST**
  Mit dieser Nachricht bestätigt ein DHCP-Client eine IP-Adresse, die entweder gerade angefordert wurde oder aktuell noch vom Client verwendet wird. Im ersten Fall wird die Nachricht wieder als Multicast-Paket versendet, im zweiten Fall als Unicast-Paket.

- **DHCPACK**
  Der DHCP-Server schickt dem Client diese Nachricht als Bestätigung für eine erfolgreich zugeteilte Lease dem Client schicken. Auch diese Nachricht wird als Multicast-Paket versendet, wenn der Client keine eigene IP-Adresse besitzt.
- **DHCPNAK**
  Genauso wie der Server eine erfolgreich zugeteilte IP-Adresse mit einem DHCPACK bestätigt, kann er eine nicht erfolgreiche Zuteilung mit einer DHCPNAK Nachricht beantworten, um den Client darüber zu informieren.
- **DHCPDECLINE**
  Wenn ein Client eine IP-Adresse von einem DHCP-Server erhält, prüft dieser, ob die Adresse schon in Verwendung ist. Er versendet dazu ein ARP-Broadcast-Paket in das Netzwerk und wartet auf eine Antwort. Erhält der Client eine Antwort, ist die IP-Adresse bereits in Verwendung und er sendet dem DHCP-Server eine DHCPDECLINE-Nachricht, damit dieser die IP-Adresse als verwendet markieren kann. Er wird diese Adresse dann nicht mehr vergeben, da sie entweder im Geltungsbereich eines anderen DHCP-Server liegt oder manuell auf einem Computer konfiguriert wurde.
- **DHCPRELEASE**
  Der DHCP-Client kann eine Lease vorzeitig freigeben, damit der DHCP-Server seine IP-Adresse wieder verwenden kann. Er sendet dazu eine DHCPRELEASE-Nachricht an den DHCP-Server, der die IP-Adresse vermittelt hat. Der Server wird diese Nachricht nicht bestätigen und erhält sie als IP-Unicast-Paket.
- **DHCPINFORM**
  Diese Nachricht kann dazu verwendet werden, Informationen von einem DHCP-Server zu erhalten, ohne eine IP-Adresse zugeteilt zu bekommen (z.B., weil der Client schon eine manuell konfigurierte IP-Adresse besitzt und lediglich die Adresse des DNS-Server wissen möchte)

Funktionsweise von DHCP

Erstmaliges Anfordern einer IP-Adresse

Damit ein DHCP-Client eine IP-Adresse von einem DHCP-Server erhalten kann, sendet er eine DHCPDISCOVER-Nachricht in das Netzwerk.
Ist ein DHCP-Server vorhanden, versendet dieser eine DHCPOFFER-Nachricht und der Client wird nun entweder keine, eine oder mehrere DHCPOFFER-Nachrichten empfangen. Empfängt er keine, wird er es maximal dreimal versuchen und dann die Autokonfiguration mit Hilfe von *APIPA* starten. Werden eine oder mehrere DHCPOFFER-Nachrichten empfangen, wählt der Client das beste Angebot und bestätigt dieses mit einer DHCPREQUEST-Nachricht. Der betroffende DHCP-Server wird daraufhin mit einer DHCPACK- oder DHCPNAK-Nachricht antworten. Im positiven Falle einer DHCPACK-Nachricht verwendet der Client die ihm zugeteilte IP-Adresse.

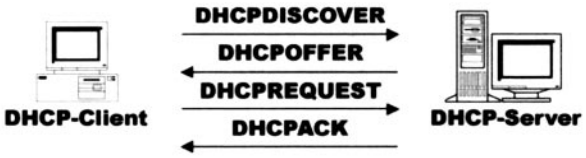

Abbildung 2-15 „Während der ersten Anforderung einer Lease ausgetauschte DHCP-Nachrichten" [LEE00]

Verlängern einer Lease für eine bestehende IP-Adresse

Der Client wird ab der Hälfte der maximalen Dauer einer Lease versuchen, diese zu erneuern. Dazu sendet er eine DHCPREQUEST-Nachricht an den DHCP-Server, der die Lease vergeben hat. Dieser antwortet entweder mit einer DHCPACK- oder DHCPNAK-Nachricht, womit die Lease als verlängert oder verweigert gilt.
Wird die Lease verweigert oder sollte sich der Computer zum Zeitpunkt der Verlängerung in einem neuen Netzwerk befinden (z.B. bei einem Laptop), wird der Client versuchen, mit einer DHCPDISCOVER-Nachricht eine neue Lease anzufordern.

Abbildung 2-16 „DHCP-Nachrichten während einer Lease-Erneuerung" [LEE00]

Beenden einer Lease

Wird die IP-Adresse vom Client nicht mehr benötigt, sendet dieser eine DHCPRELEASE-Nachricht an den DHCP-Server und gibt die IP-Adresse damit frei. Der DHCP-Server kann diese dann neu vergeben. Eine Bestätigung für die Freigabe erhält der Client vom Server nicht.

Automatic Private IP Addressing (AIPA)

Ist kein DHCP-Server vorhanden oder ist dieser ausgefallen, versucht der DHCP-Client einige Male eine IP-Adresse zu bekommen, bevor er *Automatic Private IP Addressing (AIPA)* verwendet. AIPA wählt eine eigene IP-Adresse, die aus einem speziellen IP-Adressbereich stammt, der von der IANA[23] dafür reserviert wurde. Das verwendete Netzwerk ist das Klasse B-Netzwerk 169.254.0.0 mit der Netzwerkmaske 255.255.0.0. Der DHCP-Client wählt aus diesem Bereich eine zufällige Adresse aus und überprüft mit einem ARP-Paket, ob die Adresse schon verwendet wird. Sollte dies der Fall sein, werden insgesamt 10 Versuche unternommen, um eine zufällige Adresse auszuwählen.
Fällt der DHCP-Server aus oder ist gar kein DHCP-Server vorhanden, können sich die DHCP-Clients trotzdem IP-Adressen zuweisen und miteinander kommunizieren. Da allerdings weder Gateways noch DNS-Server ermittelt werden können, ist diese Technik nur als Notlösung verwendbar.

23 Die IANA ist die zentrale Vergabestelle der im Internet verwendeten IP-Adressen.

DHCP-Relay-Agenten

Sendet ein DHCP-Client eine Anforderung für eine IP-Adresse, verwendet er dafür Multicast-Pakete, die nicht über Router weitergeleitet werden. D.h., dass in jedem Teilnetz ein eigener DHCP-Server zu Verfügung stehen müsste, der die Adressen für sein Teilnetz vergibt. Ein *DHCP-Relay-Agent* ist in der Lage die Broadcast-Pakete zu empfangen und die Anfragen an einen anderen DHCP-Server in einem anderen Teilnetz weiterzuleiten.
Der DHCP-Server kann eine IP-Adresse zuteilen und schickt diese an den DHCP-Relay-Agenten zurück, der dem DHCP-Client diese Daten übermittelt. Durch die Verwendung von DHCP-Relay-Agenten in den Teilnetzen muss nur ein DHCP-Server verwendet werden und die Konfiguration der IP-Adressen kann zentral erfolgen. Die Relay-Agenten müssen lediglich die IP-Adresse des DHCP-Servers wissen und vermitteln die Anfragen über Netzwerkgrenzen hinweg.

Aktualisierung von DNS-Einträgen

Die Verwendung von zugewiesenen IP-Adressen durch einen DHCP-Server hat den Nachteil, dass ein Client nicht unbedingt immer die gleiche IP-Adresse zugewiesen bekommt und die Konfiguration eines DNS-Servers manuell angepasst werden müsste.
Um dieses Problem zu beheben, wird in Windows 2000 das in [RFC2136] definierte Protokoll für *dynamische DNS-Aktualisierungen* verwendet. Damit kann ein DNS-Server durch einen Client aktualisiert werden und die manuelle Anpassung entfällt.
Für die Anpassung ist normalerweise der DHCP-Server verantwortlich. Der DHCP-Client sendet seinen DNS-Namen mit der DHCPREQUEST-Nachricht, so dass der DHCP-Server, der die IP-Adresse vergibt, diese an den DNS-Server senden kann. Die Aktualisierung wird sowohl für die *Forward-* als auch für die *Reverse-Lookupzonen* vorgenommen, bei Verwendung von DHCP-Clients unter Windows 2000 können diese die Einträge auf dem DNS-Server selbst aktualisieren. Damit dies funktioniert, muss der DNS-Server dynamische Aktualisierungen zulassen und Forward- und Reverse-Lookupzonen enthalten, die für dynamische Aktualisierungen konfiguriert sind.

Zusammenfassung

Die Verwendung von DHCP zur zentralen Verwaltung und Vergabe von IP-Adressdaten erleichtert die Konfiguration von vielen Computern im Netzwerk. Windows 2000 kombiniert diese Technik mit seinem DNS-Nameserver und ermöglicht dadurch die Verwendung von DNS-Namen anstelle der bisherigen NetBIOS-Namen. Durch die Verwendung von hierarchischen DNS-Namen und durch DHCP-Relay-Agenten können auch größere Netzwerke diese Technik nutzen und zentral administriert werden.

2.2.3 NetBIOS Namensdienst und der Windows Internet Name Service (WINS)

Windows verwendet traditionell *NetBIOS* für viele seiner Netzwerkdienste. Datei-, Druckerfreigaben und Netzwerksuchen werden in Windows über NetBIOS abgewickelt. Die NetBIOS-Schnittstelle bietet dafür einige Funktionen, die von den Anwendungen verwendet werden. Der Transport von Daten über ein Netzwerk kann mit NetBIOS über viele Netzwerkprotokolle, wie NetBEUI, IPX und TCP/IP, ablaufen. [RFC1001] und [RFC1002] beschreiben die NetBIOS-Dienste über das TCP/IP-Transportprotokoll, die auch einen Namensdienst beinhalten.

Neben dem NetBIOS-Namensdienst, der mit Hilfe von Broadcasts Namen im Netzwerk registriert und ausfindig macht, gibt es noch den Windows Internet Name Service (WINS) der zur Namensregistrierung und -auflösung einen WINS-Server verwendet. Diese beiden Namensdienste werden in diesem Kapitel erläutert.

NetBIOS-Namen und NetBIOS-Namenssuffixe

[RFC1001] und [RFC1002] definieren einen *NetBIOS-Namen* mit einer maximalen Länge von 16 Zeichen, wobei das erste Zeichen kein „*" sein darf und Groß- und Kleinschreibung nicht unterschieden wird. Mit Hilfe dieser Namen werden Netzwerkressourcen und Endknoten beschrieben und ausfindig gemacht, die von den NetBIOS-Transportdiensten verwendet werden.
Der *NetBIOS-Namensraum* ist im Gegensatz zum DNS-Namensraum flach. Die doppelte Verwendung eines Namens im Netzwerk ist nicht gestattet, wodurch die Verwaltung von vielen Computern und Diensten schwierig werden kann. Der letzte Buchstabe des NetBIOS-Namens kann außerdem nicht frei verwendet werden, er gibt den *NetBIOS-Namenssuffix* an, identifiziert den Typ der benannten Ressource und kann mit den Ressourceneinträgen des DNS-Servers verglichen werden. Ist der verwendete NetBIOS-Name kürzer als 15 Zeichen, werden die restlichen Zeichen mit Leerzeichen aufgefüllt und der Namenssuffix angehängt.
Die folgende Tabelle gibt einen Überblick über die von Windows 2000 verwendeten Namenssuffixe:

Name	NetBIOS-Suffix (hex)	Typ	Verwendung
<Computername>	00	U	Arbeitsstationsdienst
<Computername>	01	U	Nachrichtendienst
<Computername>	03	U	Nachrichtendienst
<Computername>	20	U	Serverdienst
<Benutzername>	03	U	Nachrichtendienst
<Domäne>	00	G	Domänenname
<Domäne>	1B	U	Hauptsuchdienst der Domäne
<Domäne>	1C	G	Domänencontroller
<Domäne>	1E	G	Wahl des Suchdienstes
<..–_MSBROWSE_>	01	G	Hauptsuchdienst

Tabelle 2-2 „Im Windowsnetzwerk verwendete allgemeine NetBIOS-Suffixe" [LEE00]

Weitere Programme und Dienste verwenden andere Namenssuffixe. Dazu gehören Microsoft Exchange und Lotus Notes.

NetBIOS-Geltungsbereiche

Die Verwendung einer flachen Namensstruktur mit nur 15 nutzbaren Zeichen kann eine große Herausforderung für die Administration von größeren Netzwerken sein. Daher ist in [RFC1001] ein weiteres Kriterium definiert, das mit NetBIOS-Namen kombiniert werden kann: der *NetBIOS-Geltungsbereich*.

Die Verwendung des NetBIOS-Geltungsbereichs kann allerdings nur sehr eingeschränkt erfolgen. Der Geltungsbereich wird in Windows 2000 automatisch unter Verwendung der IP-Paramter eingestellt und kann nur über die Registrierung manuell verändert werden. NetBIOS hängt den Namen des Geltungsbereichs an jeden NetBIOS-Namen automatisch an, so dass auch nur NetBIOS-Namen im gleichen Geltungsbereich aufgelöst werden können. Eine Auflösung eines Namens in einem anderen Geltungsbereich ist nicht möglich, es müsste der Geltungsbereich in der Registrierung manuell verändert und nach der Auflösung wieder zurückgestellt werden, was nicht praktikabel wäre.
Der einzige Nutzen der NetBIOS-Geltungsbereiche unter Windows ist, dass sich NetBIOS-Namen in unterschiedlichen Geltungsbereichen nicht gegenseitig stören können.

Namensdienste mit NetBIOS

Der NetBIOS Namensdienst hat drei Hauptaufgaben, wenn kein WINS-Server konfiguriert ist. Die Übertragung der NetBIOS-Nachrichten erfolgt dabei mit Hilfe des UDP-Protokolls über UDP-Port 137 in Form von Multicast-Paketen.

Anmelden eines NetBIOS-Namens

Wenn eine Netzwerkressource verfügbar wird, meldet sie sich mit einem NetBIOS-Namen im Netzwerk an. Dafür muss festgestellt werden, ob der gewünschte Name im Netzwerk schon verwendet wird. Zu diesem Zweck broadcastet der NetBIOS-Dienst eine *Namensregistrierungsnachricht* ins Netz und wartet auf eine *negative Namensregistrierungsantwort*, die dem NetBIOS-Dienst mitteilen würde, dass der Name schon verwendet wird. Bleibt eine solche negative Antwort aus, verwendet der NetBIOS-Dienst den Namen und verteidigt ihn.

Verteidigen von NetBIOS-Namen

Hat der NetBIOS-Dienst einen Namen erfolgreich angemeldet, wird er ihn gegenüber anderen Clients verteidigen, indem er selbst negative Namensregistrierungsantworten versendet, wenn ein anderer Client eine Namensregistrierungsnachricht für diesen Namen ins Netzwerk broadcastet.

Auflösen von NetBIOS-Namen

Soll ein NetBIOS-Name im Netzwerk aufgelöst werden, broadcastet der NetBIOS-Dienst eine *Namensanforderungsnachricht* ins Netzwerk und wartet auf eine *positive Namensabfrageantwort*, die die entsprechende IP-Adresse enthält. Sollte eine positive Antwort ausbleiben, wird diese Anfrage mehrere Male durchgeführt.

Namensdienste mit WINS

Der *WINS-Dienst* erweitert nun diesen auf Broadcasts gestützten Namensdienst durch einen *WINS-Server* und *-Client*. Der WINS-Server übernimmt dabei die Aufgabe, die Namensregistrierung zentral durchzuführen und diese auch über IP-Netzwerkgrenzen hinweg zu ermöglichen, da für die Anfrage und Registrierung von Namen Unicast-Pakete zum WINS-Server gesendet werden. Auch diese verwenden UDP und Port 137.

Für die Verwendung eines NetBIOS-Namensdienst mit WINS definieren]RFC1001] und [RFC1002] folgende Typen von Endknoten:

- **B-Knoten (B-Node, Broadcast - Node)**
  Dieser Endknoten verwendet für die Namensauflösung und -registrierung ausschließlich die Broadast-Methode und keine WINS-Dienste. Dies ist der Standardknotentyp für Windows 2000 Computer, die nicht für die Verwendung von WINS-Servern konfiguriert sind. Microsoft verwendet einen angepassten B-Knoten, der um einen NetBIOS-Namenscache und eine LMHOSTS-Datei erweitert wurde. Der Namenscache wird für kürzlich aufgelöste NetBIOS-Namen verwendet und verringert den Netzwerktraffic. Die LMHOSTS-Datei entspricht in ihrer Funktion der HOSTS-Datei eines DNS-Clients und kann eine Liste von NetBIOS-Namen und deren IP-Adressen enthalten. Die LMHOSTS-Datei muss sich dafür im Verzeichnis <system-root>\system32\drivers\etc befinden.
- **P-Knoten (P-Node, Point to Point - Node)**
  Dieser Endknoten verwendet ausschließlich WINS-Dienste für die Namensauflösung und Registrierung. Dieser Knotentyp kann eingesetzt werden, wenn Broadcasts im Netzwerk vermieden werden sollen.
- **M-Knoten (M-Node, Mixed - Node)**
  Ein M-Knoten wird für die Namensregistrierung und -auflösung zuerst Netzwerk-Broadcast und, wenn dies keinen Erfolg hatte, den WINS-Server verwenden. Dieser Knotentyp ist sinnvoll, wenn sich der WINS-Server in einem entfernten Netzwerk befindet und nicht für jede Abfrage verwendet werden soll.
- **H-Knoten (H-Node, Hybrid - Node)**
  Dieser Knoten verwendet zuerst den WINS-Server für Auflösung und Registrierung von Namen und danach die Broadcast-Methode. Dieser Knotentyp ist der Standardknoten für Windows 2000 Computer mit konfiguriertem WINS-Server.

Windows 2000 Clients sind normalerweise B- oder H-Knoten, je nachdem ob WINS-Server im System konfiguriert sind oder nicht. Diese Einstellung kann allerdings manuell in der Registrierung („HKLM\SYSTEM\CurrentControlSet\Services\Netbt\Parameters“ oder „HKLM\SYSTEM\CurrentControlSet\Services\Netbt\Adapters\Interfaces\<interface>“) geändert werden. Dazu muss ein neuer „NodeType“-Wert vom Typ REG_DWORD erzeugt werden. Die Werte 1,2,4 und 8 repräsentieren die B-, P-, M- und H-Knoten.

Namensregistrierung mit WINS

Der Registrierungsvorgang eines NetBIOS-Namen ist vom Endknotentyp abhängig. Während ein B-Knoten nur durch Broadcasts den Namen im Netzwerk registriert, sendet ein Client vom Typ P ein Unicast-Paket an den WINS-Server. Sollte der Name am WINS-Server schon registriert sein, testet der Server, ob der momentane Besitzer des Namens noch im Netzwerk erreichbar ist. Ist dies der Fall, sendet der WINS-Server eine negative Namensregistrierungsnachricht an den Client, der den Namen registrieren wollte. Ist der Name nicht registriert oder meldet sich der ehemalige Besitzer nicht auf die Anfrage, sendet der WINS-Server eine positive Namensregistrierungsnachricht an den Client. Der Server kann außerdem noch eine Abwartebestätigungsnachricht an den Client senden, wenn er für die Verarbeitung der Anfrage noch etwas Zeit benötigt.

Ein NetBIOS-Client vom Typ M wird zuerst mit Hilfe von Broadcasts versuchen, den Namen zu registrieren und im Falle eines Erfolges sich bei einem WINS-Server registrieren. NetBIOS-Clients vom Typ H versuchen, sich nur am WINS-Server zu registrieren und verwenden keine Broadcasts.

Namenserneuerungsanforderung und Gültigkeitsdauer der Namen (TTL)

Die registrierten Namen haben nur eine begrenzte Lebensdauer. Der WINS-Server wird die Namen nur für eine bestimmte Zeit registrieren und auflösen (normalerweise 6 Tage) und dann den Namen freigeben. Windows 2000 Clients versuchen daher, nach der Hälfte der Zeit und nach einem Neustart den Namen zu erneuern.
Dazu sendet der Client eine Namenserneuerungsanforderung an den WINS-Server. Dieser wird die Nachricht mit einer positiven oder negativen Namensregistrierungsnachricht bestätigen.

Namensfreigabe

Ein NetBIOS-Client kann einen registrierten Namen aktiv bei seinem WINS-Server freigeben. Dazu sendet er eine *Namensfreigabeanforderung* an den WINS-Server, der die Freigabe mit einer *Namensfreigabeantwort* bestätigt.

WINS-Namensauflösung

Zur Namensauflösung sendet ein NetBIOS-Client, der mit einem WINS-Server konfiguriert wurde, eine Namensabfragenanforderung an seinen WINS-Server, der dann versucht den Namen aufzulösen. M-Knoten verwenden allerdings zuerst die Broadcast-Methode und erst dann den WINS-Server, während H-Knoten zuerst den WINS-Server verwenden.
Ein WINS-Server wird eine Anforderung entweder mit einer positiven oder einer negativen Namensabfrageantwort an den Client beantworten. Eine positive Antwort enthält dann die gewünschte Adresse.

NetBIOS-Namensauflösung von Windows 2000

Windows 2000 verwendet für eine Namensauflösung eine Reihe von Methoden gleichzeitig, um die Wartezeit möglichst zu minimieren. So werden zuerst die lokalen Caches von NetBIOS und vom DNS nach dem Namen durchsucht, sowie HOSTS- oder LMHOSTS-Dateien verwendet. Der nächste Schritt ist eine DNS- und dann eine NetBIOS-Abfrage, die je nach Knotentyp entweder Broadcasts, einen WINS-Server oder beides verwendet.

WINS-Proxy

Ein *WINS-Proxy* kann verwendet werden, wenn einige NetBIOS-Clients nicht für die Verwendung von WINS-Servern konfiguriert sind, aber trotzdem ein WINS-Server eingesetzt werden soll. Der WINS-Proxy verhält sich dann wie ein B-Knoten, verteidigt aber alle NetBIOS-Namen, die im WINS-Server registriert sind. Wenn ein NetBIOS-Client versucht, einen Namen mit Broadcast-Paketen zu registrieren, wird der WINS-Proxy beim WINS-Server nachfragen, ob der Name schon registriert wurde. Sollte dies der Fall sein, wird er den Namen wie ein B-Knoten verteidigen und eine negative Namensregistrierungsnachricht zurück ins Netzwerk broadcasten. Bei einer Namensauflösung wird ein WINS-Proxy über Broadcasts die Namen auflösen, die der WINS-Server auflösen kann, so dass Namen, die nur im WINS-Server gespeichert sind, auch von B-Knoten aufgelöst werden können.

Um ein System als WINS-Proxy zu konfigurieren, muss der folgende Registrierungsschlüssel editiert werden:

HKLM\SYSTEM\CurrentControlSet\Services\Netbt\Parameters bzw.
HKLM\SYSTEM\CurrentControlSet\Services\Netbt\Parameters\
Adapters\Interfaces\<interface>

Der Wert „EnableProxy" vom Typ REG_DWORD Boolean kann entweder False,0 (Proxy inaktiv) oder True,1 (Proxy aktiv) sein.

WINS-Datenreplikation

Damit größere Netzwerke WINS-Server einsetzen können, ist es sinnvoll einzelne Teilnetze mit eigenen WINS-Server auszustatten. Damit diese untereinander ihre Daten abgleichen, können diese entsprechend konfiguriert werden. Dazu werden jeweils zwei Server zu einem Paar verbunden, die ihre Daten untereinander replizieren. Es gibt zwei Arten von Server innerhalb der Replikationsstruktur: *Push- und Pull-Server*. Die Art des Server hat allerdings keinen Einfluss auf die Datenübertragung, denn es werden immer Daten von einem Server abgefragt, sondern bestimmt, wer den Replikationsprozess startet. Ein Pull-Server wird in festgelegten Intervallen den Replikationsprozess starten, während ein Push-Server wartet, bis sich eine gewisse Anzahl von Änderungen ergeben. Es ist möglich und sinnvoll, die Server als Push- und Pull-Server zu konfigurieren, damit eine möglichst schnelle Synchronisation der Daten erfolgen kann.

Zusammenfassung

Die NetBIOS Namensdienste und das WINS-System sind seit geraumer Zeit die verwendeten Namensdienste in Windows-Netzwerken. Auch Windows 2000 unterstützt die alten Protokolle und verwendet parallel den Namensdienst von DNS zur Namensauflösung und Domänenverwaltung. In gemischten Netzwerken sollte also genau geplant werden, welche Dienste eingesetzt werden und welche Clients mit welchen Namensdiensten arbeiten.

2.2.4 Domain Name System (DNS)

Jeder Host in einem Netzwerk wird anhand einer eindeutigen Netzwerkadresse identifiziert. Da der menschliche User nur schwer mit solchen Nummern umgehen kann, wird er die Verwendung von Namen für häufig verwendete Computer bevorzugen. Die Auflösung der Namen in Netzwerknummern wird dabei von einem Namensdienst übernommen, der im Internet durch das Domain Name System (DNS) realisiert wird.
In den Anfängen des Arpanet [24]wurden alle Hosts in einer Textdatei hosts.txt geführt. In dieser Datei stand der Name und die Netzwerknummer von jedem Computer, der an das Netzwerk angeschlossen war. Diese Datei wurde nach einer Veränderung an alle an das Netzwerk angeschlossenen Hosts übertragen, damit diese eine aktuelle Version besaßen.
Aufgrund des raschen Wachstums des Arpanet wurde die Pflege der Liste allerdings zu aufwendig und ein neues System sollte die Namensauflösung übernehmen. Folgende Kriterien sollte das neue System dabei erfüllen:

---

24 Das Arpanet (Advanced Research Projects Agency) ist der Vorläufer vom heutigen Internet

- **Hierarchische Namensraum**
  Die Verwendung einer hierarchischen Struktur vereinfacht die Zuordnung von Hostnamen zu Gruppen in Form von Domänen. Jede Domäne kann weitere Domänen enthalten und gehört zu einer übergeordneten Domäne, mit Ausnahme der Stammdomäne, die keine weitere übergeordnete Domäne enthält.
- **Verteilte Verwaltung der Datenbank**
  Die frühere host.txt Datei wurde zentral verwaltet. Das neue System sollte die Möglichkeit einer dezentralen Verwaltung bieten, damit die Pflege vereinfacht wird.

Das neue System wurde in [RFC0882] und [RFC0883] veröffentlicht, in [RFC1034] und [RFC1035] als *DNS Dienst (Domain Name System)* vorgestellt und von der IETF standardisiert. Seitdem wird es als Namensdienst im Internet verwendet und noch immer weiterentwickelt.

Domänennamen

Das Domain Name System verwendet einen *hierarchisch aufgebauten Namensraum*, dessen einzelne *Knoten* jeweils eine Domäne darstellen und der einen namenslosen *Stammknoten* besitzt. Jeder Knoten, also jede Domäne, kann wiederum untergeordnete Knoten bzw. Domänen besitzen. Jeder Knoten besitzt einen Namen, der in [RFC1034] als Label oder DNS-Bezeichnung benannt wird und aus 1 bis 63 Zeichen bestehen kann. Jeder Knoten erhält nun seinen Domänennamen durch Aneinanderreihung der DNS Bezeichnungen bis hinauf zum Stammknoten, wobei die Namen durch Punkte getrennt werden. Der Knoten „Firma" der dem Knoten „com" untergeordnet ist, wobei der Knoten „com" direkt mit dem Stammknoten verbunden ist, erhält also den Domänennamen „Firma.com", der auch als vollständig bezeichneter Domänenname *(Fully Qualified Domain Name, FQDN)* bezeichnet wird.

Top-Level-Domänen

Die direkt unterhalb des Stammknotens angeordneten Domänen werden auch als *Top-Level-Domains (TLDs)* bezeichnet. Es gibt folgende Gruppen von TLDs:

Top-Level-Domains mit drei Buchstaben

Diese TLDs sind in [RFC1591] definiert und werden für unterschiedliche Verwendungszwecke eingesetzt:

com	Kommerzielle Organisationen
edu	Organisationen aus dem Bildungsbereich (Schulen, Universitäten)
gov	Bereiche der US-Bundesregierung
int	Internationale Organisationen
mil	US-Militär
net	Organisationen, die mit der Verwaltung des Internets beschäftigt sind (Provider etc.)
org	Organisationen, die in die anderen Bereiche nicht hineinpassen

Es hat sich inzwischen gezeigt, dass die strikte Einhaltung der TLDs com, net und org nicht durchgesetzt werden kann und sich z.B. auch viele kommerzielle Organisationen in der .net Domäne finden lassen, die nicht direkt mit der Verwaltung des Internets zu tun haben. Ein Grund dafür mag die immer schwieriger werdende Suche nach freien Domänennamen sein, wodurch der Bedarf an weiteren Top-Level-Domänen immer größer wird.

Länderspezifische Top-Level-Domänen mit zwei Buchstaben

Durch Nutzung der ISO-Ländercodes erhält jedes Land seine eigene Domäne, dessen Verwaltung dem Land unterliegt. Beispiele für diese TLDs sind de für Deutschland, it für Italien und se für Schweden.

Die ARPA Top-Level-Domäne

Diese Domäne wird für Reverse Lookups verwendet, die später beschrieben werden.

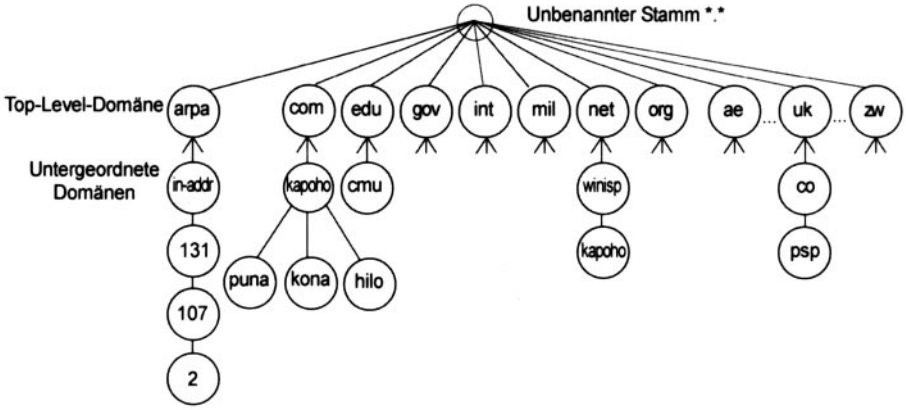

Abbildung 2-17 „Der Domänennamespace für das Internet" [LEE00]

Ressourceneinträge (RR)

Nachdem die Domänen strukturiert sind, fehlen für die sinnvolle Verwendung noch Informationen über einzelne Ressourcen in einer Domäne, die dann in Netzwerkadressen umgewandelt werden können. Diese Informationen werden in *Ressourceneinträgen* gespeichert, die einer Domäne zugeordnet sind und in zahlreichen RFCs ([RFC1035], [RFC1036] und andere) definiert werden. Mit Hilfe eines Ressourceneintrags kann nun ein Host oder ein E-Maildienst innerhalb einer Domäne lokalisiert und in eine Netzwerkadresse aufgelöst werden. Ein Domänenserver, der für eine bestimmte Domäne verantwortlich ist, verwaltet alle aktuellen Ressourceneinträge dieser Domäne. Andere Domänenserver können diese Ressourceneinträge zwischenspeichern, um einen schnellen Zugriff auf diese Einträge zu ermöglichen.
Jeder Ressourceneintrag enthält einige allgemeine Informationen. Dazu zählen die Domäne, die den RR enthält und damit Besitzer (Owner) des RRs ist und die Klasse, die früher verwendet wurde und heute generell IN (Internet) ist. Einweiterer Eintrag ist die TTL (Time to Live), die angibt, wie lange ein RR gültig ist. Andere Domänenserver, die nicht autorisierend für eine Domäne sind, dürfen den RR dann solange zwischenspeichern, wie es die TTL angibt. Ist die Zeit abgelaufen, werden diese RR vom autorisierten Domänenserver neu verlangt. Der Typ eines Ressourceneintrags bestimmt die Art der Ressource, wovon hauptsächlich folgende Verwendung finden.

- **Hostadresse (A)**
  Dieser RR verbindet einen FQDN mit einer 32bit langen IPv4 Adresse. Er stellt die Verbindung zwischen Domänennamen und Netzwerkadressen her. Alle anderen Ressourceneinträge enthalten in der Regel keine direkten Netzwerkadressen, so dass diese eigentlich immer in zwei Schritten aufgelöst werden.
- **IPv6 Hostadresse (AAAA)**
  Dieser Eintrag erfüllt den gleichen Zweck wie ein A-Eintrag, gibt allerdings eine 128bit lange IPv6 Adresse zurück.
- **Kanonischer Name (CNAME)**
  Ein CNAME-Eintrag ist ein Alias für einen FQDN. So können Netzwerkressourcen, wie entfernte Host, mit einem Aliasnamen im DNS eingetragen werden. Ändert sich der richtige FDQN, muss nur der CNAME Eintrag lokal geändert werden. Eine weiteres Einsatzgebiet ist die Verwendung von kürzeren Namen für häufig genutzte Ressourcen.
- **Mail Exchanger (MX)**
  Dieser Eintrag bestimmt einen oder mehrere Mailserver, die für diese Domäne E-Mails annehmen. Er enthält die Namen der Mailserver, die über A-Einträge aufgelöst werden können, und jeweils einen zugeordneten Referenzwert, über den die Reihenfolge der Mailserver bestimmt wird.
- **Nameserver (NS)**
  Er enthält eine Auflistung von autorisierenden Namensserver für diese Domäne und deren delegierte Subdomänen.
- **Pointer (PTR)**
  Dieser spezielle Eintrag wird hauptsächlich für Reverse-Lookups verwendet, d.h., um eine IP Adresse in einen Domänennamen aufzulösen.
- **Start of Authority (SOA)**
  Der SOA-Eintrag zeigt den primären Namensserver für diese Domäne an. Dieser Eintrag enthält außerdem noch weitere Informationen über eine Domäne.
- **Service Locator (SRV)**
  Der Service Locator wird dazu verwendet, bestimmte Dienste, wie z.B. einen Active Directory Domänencontroller, ausfindig zu machen. Dieser Typ wird unter Windows 2000 hauptsächlich dazu verwendet, das Active Directory zu unterstützen.

Zonen

Um die Verwaltung der Domänen weiter zu vereinfachen, sind diese in *Zonen* aufgeteilt. Eine Zone enthält nun die zu einer Domäne zugehörigen Ressourceneinträge. Es können auch weitere Subdomänen und deren RRs einer Zone zugehören.

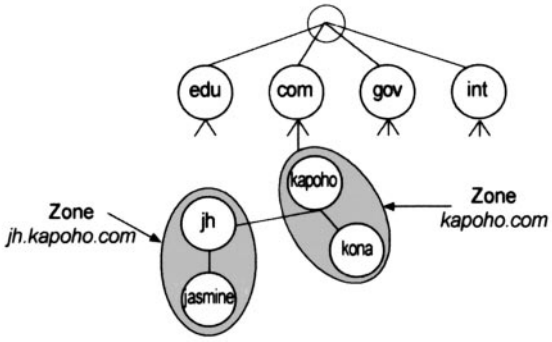

Abbildung 2-18 „Zonen und Domänen" [LEE00]

Sollen Subdomänen von einer anderen Instanz verwaltet werden, werden diese an eine untergeordnete Zone delegiert und auf einem anderen DNS-Server verwaltet. Die Delegierung einer Zone ermöglicht die verteilte Verwaltung des Domain Name System. Es gibt drei verschiedene Zonentypen, die auf einem Windows 2000 Server eingesetzt werden:

- **Primärer Standardtyp**
  Dieser Zonentyp entspricht der normalen primären Zone im Domain Name System. Alle verwaltungstechnischen Aufgaben werden in dieser Zone vorgenommen, da diese Zone autorisierend für die enthaltenen Domänen ist. Diese Zone enthält außerdem den SOA-Eintrag, um sich als primäre Zone zu identifizieren. Um Redundanzen zu erzeugen, kann die primäre Zone automatisch an eine oder mehrere sekundäre Zonen verteilt werden.
- **Sekundärer Standardtyp**
  Eine sekundäre Zone ist eine schreibgeschützte Kopie einer primären Zone. Die Daten der Zone werden durch einen Zonentransfer auf die sekundäre Zone repliziert. Dadurch wird die Leistungsfähigkeit des DNS erhöht, da mehrere Server Anfragen für diese Zone bearbeiten können. Die Häufigkeit der Replikation wird durch den SOA-Eintrag der primären Zone bestimmt. Das bedeutet allerdings auch, dass eine Änderung an einer primären Zone oft erst nach einigen Stunden auf den sekundären Server repliziert wird.
- **Active Directory integrierter Zonentyp**
  Dieser von Microsoft eingesetzte primäre Zonentyp verwaltet die Zoneninformationen im Active Directory. Die Replikation der Zoneninformationen wird mit Hilfe der Active Directory-Replikation durchgeführt.
  Der Vorteil liegt darin, dass die Änderung der Zoneninformationen auf mehreren Servern erfolgen kann und diese über die Active Directory-Replikation auf andere Server synchronisiert werden. Ein weitere Vorteil besteht in der effektiveren Übertragung der Zoneninformationen während der Replikation, da diese komprimiert werden.

Reverse-Lookupzonen

Normale Abfragen an das DNS System basieren auf Domänennamen und Ressourceneinträgen und erwarten vom DNS als Antwort eine IP Adresse oder einen Domänennamen für einen bestimmten Zweck.

Dieser spezielle Zonentyp wird für die umgekehrte Auflösung von IP Adressen nach Domänennamen verwendet und beantwortet Abfragen wie „Welcher Domänenname gehört zu 212.123.45.67?". Dafür wurde eine spezielle Domäne „in-addr.arpa" eingerichtet, die PTR Einträge für die entsprechenden IP Adressen, die umgewandelt werden können, enthält. IP-Adressen werden in Domänennamen umgewandelt und im DNS verwaltet. Die einzelnen Zahlen einer IP-Adresse werden umgekehrt geschrieben und mit der in-addr.arpa Domäne verbunden. Aus der Adresse 192.168.1.20 wird daher der Eintrag „20.1.168.192.in-addr.arpa" und aus dem Teilnetz 192.168.2.0 der Eintrag „2.168.192.in-addr.arpa". Dadurch ist es möglich, auch Teilnetze als Subdomänen zu interpretieren und an andere Zonen zu delegieren. Die Domäne „in-addr.arpa" wird allerdings nur für IPv4 basierende IP-Adressen benutzt. IPv6 benutzt für Reverse-Lookupzonen die Domäne „ip6.int".

Die 13 Stammserver

Die Aufteilung in Zonen ermöglicht die Aufteilung der Verwaltung und Verantwortung der Ressourceneinträge der Domänen. Im Internet befinden sich zu diesem Zweck 13 *Stammserver* (a.root-servers.net bis m.root-servers.net), die alle Informationen über die Top-Level-Domänen com, net, org sowie die länderspezifischen Domänen verwalten. Diese Stammserver delegieren alle weiteren Subdomänen an entsprechende DNS-Server, so dass ein Internethost in der Lage ist, alle Domänennamen aufzulösen.

Hauptkomponenten des DNS-Systems

Die beiden Hauptkomponenten des DNS sind der DNS-Server und der *DNS-Resolver* der im DNS-Client die Aufgabe der DNS-Abfrage übernimmt. Zu diesem Zweck muss im Clientsystem mindestens ein DNS-Server eingetragen werden.
Unter Windows 2000 ist der DNS-Resolver ein Teil des DNS-Clientdienstes, der automatisch mit TCP/IP mitinstalliert wird und sich mit dem Windows 2000 Systemkonto an das System anmeldet. Der DNS-Resolver besitzt einen Cache-Speicher, der bei mehrmaligen Anfragen eines RRs eines Domänennamen verwendet wird. Dadurch wird die Anzahl der Anfragen im Netzwerk reduziert und die Leistung erhöht. Der *DNS-Resolvercache* speichert die empfangenen Ressourceneinträgen solange, wie es die TTL (Time to Live) im RR erlaubt. Der Inhalt des Caches kann mit Hilfe des Befehls ‚IPCONFIG /DISPLAYDNS' angezeigt werden.
Zusätzlich verwendet der DNS-Resolver eine Negativliste, die alle RRs enthält, die nicht aufgelöst werden konnten. Diese werden in der Negativliste 300 Sekunden lang gespeichert. Damit wird das mehrmalige Abfragen von RRs und Domänennamen verhindert, wenn diese nicht aufgelöst werden konnten. Die Standardzeit von 300 Sekunden kann unter Windows 2000 in der Registrierung über den Registrierungseintrag „NegativeCacheTime" unter HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Paramteres eingestellt werden.
Sollte überhaupt kein DNS Server antworten, werden alle weiteren DNS Abfragen für 30 Sekunden sofort negativ beantwortet, um unnötigen Netzwerkverkehr zu verhindern.

Dynamisches DNS

DNS-Zonen können aktualisiert werden. Diese Technik wird in [RFC2136] beschrieben. Damit sind DNS-Clients in der Lage, ihre RRs auf dem DNS-Server selbständig zu aktualisieren. Unter Windows 2000 verwendet der DNS-Client und der DHCP-Server *dynamische DNS Aktualisierung*, um die RRs des DNS-Servers zu aktualisieren. Erhält ein Windows 2000 Client beispielsweise eine neue IP-Adresse vom DHCP-Server, so aktualisiert der DNS-Client automatisch die Ressourceneinträge im DNS-Server.

Rekursive und Iterative Abfragen

DNS-Abfragen können entweder rekursiv oder iterativ sein. Normalerweise stellt ein DNS-Client eine rekursive Anfrage an einen DNS-Server. Kann der Server nicht selbst die Anfrage beantworten, wird er damit beginnen, iterative Anfragen an andere DNS-Server, z.B. die Stammserver, zu richten, um eine Antwort zu erhalten, die er dann an den Client zurücksenden kann.
Bei einer iterativen Abfrage wird der DNS-Server nur in seiner eigenen Datenbank suchen und die entsprechende Antwort zum DNS-Client oder einen anderen DNS-Server zurückschicken. Daher wird die iterative Abfrage hauptsächlich von DNS-Servern benutzt.

Zonentransfer

Es ist üblich, dass eine Zone nicht nur auf einem primären DNS-Server gespeichert wird, sondern dass es einen oder mehrere DNS-Server gibt, die von dieser Zone eine Kopie gespeichert haben und diese als sekundäre Zone im DNS eingetragen ist. Dadurch können Abfragen auch von den sekundären DNS-Server beantwortet werden.
Allerdings müssen sekundäre DNS-Server dafür sorgen, dass sie immer eine aktuelle Kopie der primären Zone gespeichert haben. Die Übertragung der Informationen wird *Zonentransfer* genannt. In regelmäßigen Abständen, die im SOA-RR als TTL eingetragen sind, prüft der sekundäre DNS-Server, ob sich die Zonendaten geändert haben. Dafür fragt er den SOA-RR der primären Zone ab und vergleicht die Seriennummern der Zonendateien. Ist die Seriennummer auf dem primären DNS-Server höher, als die, die er selbst gespeichert hat, geht der sekundäre Server davon aus, dass sich die Zonendaten geändert haben, da jede Änderung an den primären Daten eine Erhöhung der Seriennummer bewirkt.
Die Übertragung der Zonendaten kann nun entweder komplett erfolgen, wobei der gesamte Satz an RRs übertragen wird, oder wenn beide DNS-Server dieses Protokoll unterstützen, als *inkrementeller Zonentransfer*, wie in [RFC1995] definiert, ablaufen. Dabei muss der primäre DNS-Server jede Änderung an den Zonendaten protokollieren, damit er wissen kann, welche Änderungen er dem sekundären DNS-Server übermitteln muss. Der sekundäre DNS-Server erhält dann nur die geänderten Daten, womit er seinen eigene Datenbank aktualisieren kann.

Active Directory integrierte Zonenreplikation

Zonen, die als Active Directory Zonen eingerichtet sind, verwenden die Active Directory Replikationsmechanismen. Dies hat gegenüber der herkömmlichen Zonenreplikation einige Vorteile. Zum einen können alle DNS-Server, die die Active Directory Zone teilen, Änderungen an der Zone vornehmen. Diese werden dann auf alle anderen DNS Server automatisch durch das Active Directory

repliziert. Zum anderen ist die Active Directory Replikation effizienter, da nur geänderte Daten (wie beim inkrementellen Zonentransfer) übertragen und vor der Übertragung komprimiert werden. Werden allerdings gemischte Systeme verwendet, d.h. DNS-Server anderer Hersteller, kann die AD-Replikation nicht verwendet werden, da die DNS-Server anderer Hersteller die AD-Replikation nicht unterstützen.

Zusammenfassung

Windows 2000 verwendet das DNS nicht nur zur Verwaltung von Hostadressen für Internetdienste. Die gesamte Domänenstruktur von Windows 2000 basiert auf den DNS-Dienst, der als Datenspeicher das Active Directory verwendet. Dafür wurden neue Zonentypen, die das Active Directory unterstützen, hinzugefügt und dynamisches DNS ermöglicht den Update von Informationen durch einen Client.

2.2.5 FileServer (Datei- und Druckerfreigabe)

Windows 2000 bietet auf einfache Art und Weise die Möglichkeit, Ressourcen im Netzwerk freizugeben. Dafür wird das *Common Internet File System* (CIFS) verwendet, das eine Erweiterung des *Server Message Block* (SMB) ist. Die Namensänderung wurde vorgenommen, um es zu einem „offenen" Protokoll zu machen, das der Effektivität halber in einer höheren Netzwerkebene als NetBIOS liegt. Meist wird es für Datei- und Druckerfreigaben eingesetzt, es kann aber auch für IPC *(Inter-Process Communication)* genutzt werden, um die Kommunikation zwischen Prozessen auf verschiedenen Systemen zu ermöglichen und so beispielsweise die Zusammenschaltung für Berechnungen in einer Anwendung auf mehreren Computern zu Zeiteinsparungszwecken zu ermöglichen.

Ein weiterer Netzwerkdienst, der allerdings nur in den Windows 2000 Server Versionen verfügbar ist, ermöglicht Datei- und Druckdienste für Unix- und Apple-Macintosh-Rechner. Mit Hilfe dieser Dienste wird es möglich, das Windows-Netzwerk an Protokolle wie AppleTalk von Apple anzupassen und damit beispielsweise aus einem Windows-Dateiserver auch einen Server für Apple-Rechner zu machen, die in ihrer gewohnten Umgebung auf so einen Server zugreifen können. Zusätzlich ist die Installation von Serversoftware durch Fremdanbieter möglich, um auch anderen Plattformen den Zugriff zu ermöglichen.

Die Verwaltung der Freigaben für Netzwerkordner auf den einzelnen Rechnern bleibt den Benutzern vorbehalten und sie können für einzelne Objekte Zugriffsberechtigungen einrichten. Dabei können sie entscheiden, wer auf welche Objekte zugreifen darf, ob dafür Passwörter nötig sind und welcher Art der Zugriff ist.

SMB über NetBIOS benutzt Port UDP / 137 (NetBIOS name service) und UDP / 138 (NetBIOS datagram service) oder TCP / 139 (NetBIOS session service). Es ist auch möglich, SMB ohne NetBIOS zu benutzen, und zwar über TCP / 445. Dies wird als *Direct Host* bezeichnet und ist neu in Windows 2000.

Der SMB-Dateisystem-Treiber enthält zwei Komponenten, die die Dateifreigabe ermöglichen. Den *SMB Redirector*, der mit der SMB Server-Komponente auf dem verbundenen System kommuniziert und unter anderem vom Workstation-Dienst genutzt wird. Und den *SMB Server*, bei dem der *Server-Dateisystem-Treiber* und der *Server-Dienst* für die Verbindungen, die von Client-Seite angefordert werden, arbeiten und die Anfragen an den *Dateisystem-Treiber*, in Falle von Windows 2000 FAT,FAT32 oder NTFS, weiterleiten.

2.2.6 Internet Information Server (IIS) 5.0

Der Internet *Information Server (IIS)* wird häufig als der Webserver von Windows NT bzw. Windows 2000 angesehen. Auch wenn dies meistens das Haupteinsatzgebiet ist, sind noch eine Reihe weiterer Funktionen im IIS integriert. Dazu zählen der *FTP-* und der *SMTP- Server*, aber auch weitere Protokolle und Dienste, wie z.B. das *WebDAV-Protokoll*, die einen ganz erheblichen Einfluss auf die Sicherheit eines Windows 2000 Systems haben können.
Der IIS wird auf allen Windows 2000 Serverversionen automatisch installiert, auf Windows 2000 Clients kann der IIS manuell installiert werden. Beide Versionen des IIS sind identisch, der IIS auf einem Windows 2000 Client ist allerdings in der Leistung begrenzt, so dass er nur für kleinere Projekte oder Testumgebungen eingesetzt werden kann.
Der IIS ist eng mit anderen Systemdiensten verbunden. So benutzt der Webserver zur Speicherung seiner Konfiguration das Active Directory und der Microsoft Exchange Server verwendet den IIS z.B. für den Outlook Web Access Client und andere Funktionen.
Dadurch wird es sehr schwierig, den IIS nicht zu installieren, selbst wenn keine Webdienste auf einem Server gewünscht sind, da andere Programme, wie z.B. das erwähnte Microsoft Exchange, diesen voraussetzen. Eine Auseinandersetzung mit den Funktionen und der Sicherheit des IIS ist also in den meisten Fällen notwendig.

Funktionsweise

Generell dient der IIS dazu, Informationen über Standardprotokolle, die im Internet Verwendung finden, bereitzustellen oder Daten über diese Protokolle zu empfangen und zu verarbeiten. Dabei kann die Quelle oder das Ziel der Daten sehr unterschiedlich sein. Durch die enge Verbindung des IIS mit anderen Diensten können dies z.B. Datenbanken, das Active Directory oder das Dateisystem sein. Der IIS ist also nicht nur in der Lage, Daten zu publizieren, sondern es können z.B. auch Dateien oder Programme im lokalen Dateisystem abgelegt und sogar gestartet werden. Diese Funktionen sind von großem Nutzen, sie können aber genauso viel Schaden anrichten.
Durch die integrierten Sicherheitsfunktionen von Windows 2000 und einigen weiteren, die im IIS integriert wurden, soll sichergestellt werden, dass nur berechtigte Benutzer in der Lage sind, solche Funktionen anzuwenden.

Konfiguration des IIS

Die gesamte Konfiguration des IIS kann über das *MMC Snap-In „Internet-Informationsdienste"* erfolgen, das sich in der Serververwaltung befindet. Mit dem Snap-In kann der IIS-Dienst auf einem lokalen und entfernten Server konfiguriert werden. Dadurch ist die Verwaltung mehrerer Webserver innerhalb eines Firmennetzes von einer zentralen Stelle aus möglich.

Zusätzlich kann für die entfernte Verwaltung des Internet Information Servers eine *Verwaltungswebsite* installiert werden. Diese wird über die Serverkomponenten hinzugefügt, benötigt lediglich einen Webbrowser mit JavaScript-Unterstützung und erlaubt die entfernte Verwaltung über das Internet.
Die dritte Möglichkeit der Konfiguration besteht über das *Active Directory Service Interface (ADSI)*, das eine Schnittstelle zwischen dem Active Directory und verschiedenen Programmiersprachen herstellt. Da der IIS alle Einstellungen im Active Directory speichert, können so eigene Programme oder Internetseiten erstellt werden, die die Konfiguration des IIS ändern oder auslesen.

Protokolle und Dienste des IIS

Webserverdienst (Protokoll: HTTP)

Die am häufigsten verwendete Funktion des IIS ist die Verwendung als Webserver. Dabei wird ein Teil des Dateisystems als Website zur Verfügung gestellt und kann über ein Webbrowser betrachtet werden.
Der IIS verwendet dafür einen beliebigen Ordner im Dateisystem, stellt diesen als so genanntes *Basisverzeichnis* zur Verfügung und verbindet es mit einer IP-Adresse und einer Portnummer (meistens Port 80).
Ein Benutzer kann nun seinen Webbrowser auf die IP-Adresse und den Port richten und erhält zunächst entweder ein *Standarddokument* oder eine Auflistung von Dateien und Ordnern im Basisverzeichnis. Der Webserver erlaubt die Verwendung von Standarddokumenten, die automatisch geöffnet und übertragen werden, wenn kein Dokument, sondern nur ein Ordner vom Benutzer angefordert wird, was in den meisten Fällen für das Basisverzeichnis zutrifft.
Diese Dokumente sind HTML-Dokumente, Bilder oder andere Dokumente, die ein Webbrowser darstellen kann.

Virtuelle Verzeichnisse

Die Ordnerstruktur der Website ist mit der Ordnerstruktur im Dateisystem identisch, kann allerdings durch *virtuelle Verzeichnisse* ergänzt werden. Virtuelle Verzeichnisse werden in der Verzeichnisstruktur des Basisverzeichnis hinzugefügt, können sich im Dateisystem aber an einer anderen Position befinden, wodurch Verzeichnisse mehrmals, z.B. in mehreren Websites verwendet, werden können, ohne dass die eigentlichen Dokumente dupliziert werden müssen.

Verzeichnissicherheit durch NTFS

Da der Webserver nicht nur Dokumente bereitstellen kann, sondern mit dem HTTP Protokoll und speziell mit der WebDAV-Erweiterung auch Dokumente auf dem Server gespeichert bzw. Programme oder Scripte ausgeführt werden können, muss der Zugang zu solchen Funktionen eingeschränkt werden.
Das NTFS-Dateisystem bietet die Möglichkeit, diese Zugriffsrechte für Webbesucher festzulegen und dies geschieht durch die Vergabe von Rechten an Dateien und Ordnern für verschiedene Benutzer. Da in den meisten Fällen der Benutzer einer Website anonym ist und sich nicht am Server anmeldet, bindet der IIS diese Besucher an ein spezielles Internet-Gastkonto mit dem Benutzernamen „IUSR_<computername>“, das bei der Installation des IIS angelegt wird und Mitglied der Gruppe Gäste ist. Mit diesem Benutzer können Zugriffsrechte im NTFS-Dateisystem für anonyme

Besucher eingerichtet werden. Der IIS bietet allerdings auch den nicht anonymen Zugang, vorhandene Benutzer können sich dann mit ihrem Namen und Passwort am Webserver anmelden. Auch dann gelten natürlich die Sicherheitseinstellungen, die im NTFS-Dateisystem konfiguriert sind. Liegen die Internetdokumente nicht auf einem NTFS-Datenträger, kann die Verzeichnissicherheit von NTFS nicht verwendet werden und eine Unterscheidung von Benutzern ist nicht möglich. Von der Verwendung von anderen Dateisystemen, die keine Sicherheitseinstellungen erlauben, wird daher dringend abgeraten.

Webserversicherheit

Der IIS-Webserver bietet noch weitere Möglichkeiten, den Zugriff auf Dokumente und Ordner einzuschränken. Das Schreiben von Daten auf den Server kann z.B. komplett unterbunden werden, egal welche Sicherheitseinstellungen das Dateisystem vorgibt und das Ausführen von Scripts oder Programmen kann ebenso verhindert werden. Da die meisten Administratoren nicht wollen, dass die Ordnerstruktur einer Website erkundet werden kann, ist diese Funktion normalerweise deaktiviert. Liegt im entsprechenden Ordner dann kein Standarddokument, erhält der Besucher eine Fehlermeldung. Dadurch kann das Auffinden von bestimmten Verzeichnissen verhindert werden, die Navigation innerhalb des Website kann dann nur noch durch *Hyperlinks* in Internetseiten erfolgen.

Das HTTP-Protokoll

Das *Hypertext Transfer Protokoll (HTTP)* ist ein Protokoll der Anwendungsschicht, wird für die Übertragung von Dokumenten und Ressourcen auf einem HTTP-Server verwendet und von kompatiblen Webbrowsern verstanden. Es dient hauptsächlich dazu eine Ressource (z.B. ein Dokument, ein Verzeichnis oder auch ein Drucker) anzufordern, bzw. auf den Server zu übertragen. Das HTTP-Protokoll wird seit 1990 verwendet und 1996 das erste Mal in [RFC1945] definiert (HTTP Version 1.0). Die aktuell verwendete Version des HTTP-Protokolls (Version 1.1) wird in [RFC2616] definiert.
Die Ressourcen werden innerhalb des HTTP-Protokolls mit *URIs (Uniform Resource Identifier)* angesprochen. Eine *URL (Uniform Resource Locator)* ist ein solcher URI und hat die folgende Form:

Schema://Computer:Portnummer/Pfad

Das *Schema* definiert in diesem Fall das HTTP-Protokoll. Der Computer wird in Form einer Adresse oder eines Namens (z.B. ein Name im DNS-System) angesprochen und der Pfad beschreibt den Pfad auf dem Webserver zur Ressource. Die Portnummer lautet beim HTTP-Protokoll in den meisten Fällen 80, kann aber auch geändert werden. Eine Beispiel URL wäre demnach: http://www.microsoft.com/support/. Wird die Portnummer weggelassen, verwenden die meisten Browser automatisch Port 80.

Möchte ein HTTP-Browser (Client) eine Ressource vom Server herunterladen, schickt er eine *Anforderung* an den HTTP-Server und erhält eine *Statusmeldung* als Antwort. Folgende Anforderungen sind möglich:

- **GET**
  Die GET-Anforderung wird in Verbindung mit einem URI dazu verwendet, die entsprechende Ressource anzufordern. Der Client erhält eine Antwort vom Server, die im Idealfall die angeforderte Ressource enthält. Die Statusmeldung meldet den Erfolg der Anforderung oder, falls die Übertragung nicht möglich war (z.B., weil die Ressource nicht existiert oder der Client keine Leseberechtigung hat), den Grund des Misserfolgs.
- **HEAD**
  Diese Anforderung ist mit der GET-Anforderung fast identisch. Es wird allerdings nicht die Ressource an den Client übertragen, sondern nur der Header wird zurückgesendet. Dieser enthält Daten über die Ressource, wie die Größe und das letzte Änderungsdatum. Diese Anforderung wird häufig verwendet, um das Vorhandensein einer Ressource zu testen oder um festzustellen, ob diese sich seit der letzten Anforderung geändert hat.
- **PUT**
  Diese Anforderung sendet eine Ressource zum Server, der diese dann speichern soll. Dabei wird eine Datei mit dieser Ressource angelegt oder eine vorhandene Datei überschrieben. Natürlich muss der Client die entsprechenden Zugriffsrechte auf dem Server haben, um Dateien schreiben zu können.
- **DELETE**
  Wenn der Client Daten auf dem Server lesen und speichern kann, sollte er natürlich auch die Möglichkeit haben, Ressourcen vom Server zu löschen. Die DELETE-Anforderung erfüllt genau diesen Zweck und fordert den Server auf, die Datei zu löschen, wofür natürlich wieder die entsprechenden Zugriffsrechte vorhanden sein müssen.
- **POST**
  Die POST-Anforderung schickt Informationen an eine vorhandene Ressource auf dem Server. Diese Ressource kann z.B. ein Programm oder ein Drucker sein, der die Informationen verarbeitet. Dabei wird keine neue Datei auf dem Server angelegt, sondern die Daten werden an eine vorhandene Ressource gesendet.
- **TRACE**
  Die TRACE-Anforderung sendet die Anforderung unverändert zurück zum Client und dient hauptsächlich der Fehlerdiagnose in einer Entwicklungsphase. Es werden keine Daten auf dem Server verändert oder gelesen.
- **OPTIONS**
  Fordert Informationen bezüglich der Leistungsfähigkeit eines Servers an. Es kann z.B. angefragt werden, welche Funktionen oder Anforderungen eine Ressource oder der Server erfüllen kann.
- **CONNECT**
  Die CONNECT-Anforderung wird für Proxies verwendet, um z.B. eine SSL Verbindung aufzubauen.

Statusmeldung

Der Client erhält auf seine Anforderung eine *Statusmeldung*, die angibt, ob die Anforderung Erfolg hatte oder welcher Grund für einen Misserfolg vorlag. Jeder Statusmeldung ist eine dreistellige Nummer zugeordnet, deren erste Ziffer etwas über die Art der Statusmeldung aussagt:

Referenznummer	Code	Bedeutung
1xx	Informativ	Zeigt eine provisorische Antwort an und gibt nur eine Statuszeile zurück, die den Status und optionale Header anzeigt. Im Grunde genommen ist dies die Methode des Servers, mit einer Bestätigungsnachricht zu antworten.
2xx	Erfolgreich	Der Server versteht und akzeptiert die Anforderung des Clients.
3xx	Umleitung	Der Anfordernde muss weitere Maßnahmen ergreifen, um auf die angeforderte Ressource zuzugreifen. Die Umleitung kann ohne jeden Benutzerzugriff erfolgen, wenn die in der nachfolgenden Anforderungsnachricht verwendete Methode entweder die GET- oder HEAD-Methode ist.
4xx	Clientfehler	Der Server glaubt, dass der Client einen Fehler begangen hat. Der Server sollte eine Erklärung des Fehlers liefern und anzeigen, ob dies ein permanenter oder temporärer Fehler ist. Darüber hinaus sollte der Server auf die TCP-Bestätigung für den Empfang der Fehlermeldung durch den Client warten, um die Verbindung nicht voreilig abzubauen.
5xx	Serverfehler	Der Server ist nicht in der Lage, die Anforderung auszuführen. Dem Client wird der Zugriff auf die Ressource nicht erlaubt oder ein Serverfehler ist aufgetreten. Der Server sollte eine Erklärung des Fehlers liefern und anzeigen, ob der Fehler temporär oder permanent ist.

Tabelle 2-3 „HTTP/1.1 Statuscodeklassen und deren Bedeutung" [LEE00]

Die weiteren Ziffern geben genauere Informationen über die Statusmeldung an, es können auch weitere Informationen im Header enthalten sein. Die genauen Fehlernummern sind im [RFC2616] definiert.

Benutzerdefinierte Fehlermeldungen

Der IIS erlaubt die manuelle Veränderung der Standardfehlerseiten, die mit den Statusmeldungen verschickt werden. So kann z.B. der Fehler 404 (Ressource nicht gefunden) angepasst werden und der Benutzer auf die Homepage der Website verwiesen werden. Andere Fehlermeldungen können durch die Einbindung von ASP (siehe Active Server Pages) eine automatische E-Mail an den Serveradministrator senden und ihn von dem Fehler in Kenntnis setzen.

HTTP Version 1.1

Das in [RFC2616] definierte HTTP-Protokoll mit der Version 1.1 enthält eine Reihe von neuen Funktionen, die eine bessere Leistungsfähigkeit des Protokolls versprechen. Dazu gehören zwei wichtige Funktionen:

HTTP Keep-Alive

Verwendet der Client oder der Server nur Version 1.0 des HTTP-Protokolls muss für jede Anforderung eine neue Verbindung zum Server aufgebaut werden. Die Keep-Alive Funktion lässt die Verbindung nach einer erfolgreichen Anforderung geöffnet, so dass neue Anforderungen über die

gleiche Verbindung übermittelt werden können. Dadurch wird die Leistungsfähigkeit des Server erhöht und die Übertragung von vielen Ressourcen beschleunigt.

Hostheadernamen

Der Mangel an IP-Adressen im weltweiten Internet hat zur Erweiterung des HTTP-Protokolls geführt. In Version 1.0 musste jede eigenständige Website eine eigene öffentliche IP Adresse besitzen, auch wenn diese auf nur einem Server gehostet wurden. Version 1.1 des HTTP-Protokoll unterstützt nun die Übertragung des *Hostnamen*, also die Domäne der angeforderten Ressource, im *HTTP-Header* und kann diesen auswerten. Danach kann der Server anhand dieser Information entscheiden, welche Webpräsenz mit der Anfrage gemeint ist und das entsprechende Basisverzeichnis auswählen. Da auf einem Server sehr viele eigenständige Webpräsenzen nebeneinander existieren können, muss nur noch eine einzelne IP-Adresse für alle Webpräsenzen verwendet werden. Diese Funktion steht nur bei unverschlüsselten Anforderungen zur Verfügung; wird die HTTP-Verbindung z.B. mit SSL verschlüsselt, wird auch der Header, der den Hostnamen enthält verschlüsselt und kann nicht für eine Unterscheidung verwendet werden. SSL-verschlüsselte Websites benötigen also weiterhin eine eigene IP-Adresse.

Gültigkeit und Klassifikation von Inhalten

Die durch das HTTP-Protokoll angeforderten Inhalte können klassifiziert und mit einer Gültigkeit versehen werden. Diese Informationen können von Browsern und Proxy-Servern verwendet werden, um z.B. Inhalte als nicht jugendfrei zu klassifizieren, so dass ein entsprechend konfigurierter Browser diese nicht anzeigt. Diese Klassifikation wird nach dem *Recreationel Software Advisory Council (RSAC)* Filtersystem nach Gewalt, Sex, Nacktaufnahmen und Sprache vorgenommen.
Die Gültigkeitsdauer einer Information ist für Suchmaschinen und Proxy Server interessant, diese können die gespeicherten Informationen nach Ablauf der Gültigkeit automatisch verwerfen.

Dateiserver (Protokolle: WebDAV und FTP)

Während es beim Webserver darum geht einer mehr oder weniger großen Anzahl von anonymen oder bekannten Benutzern Informationen über einen Webbrowser zur Verfügung zu stellen, bietet der IIS auch einen *Dateiserverdienst* an. Dieser ermöglicht das Laden und Speichern von Dateien auf dem Server in einer Ordnerstruktur.
Der IIS stellt dabei zwei Protokolle zur Verfügung, die entsprechende Clients voraussetzen.

FTP-Protokoll

Die erste Möglichkeit, den IIS als Dateiserver zu verwenden, besteht in der Einrichtung eines *FTP-Servers*. Der IIS unterstützt das *FTP-Protokoll* und kann wie beim Webserver Verzeichnisse aus dem Dateisystem per FTP-Protokoll freigeben. Dieses Protokoll ist in den RFCs [RFC0412], [RFC0959] und [RFC1635] definiert. Auch der FTP-Server unterstützt die Verwendung mehrerer Basisverzeichnisse, die mit virtuellen Verzeichnissen erweitert werden können. Leider bietet das FTP-Protokoll keine äquivalente Methode zu Hostheadernamen, so dass jeder FTP-Server eine unterschiedliche IP-Adresse oder einen anderen Port verwenden muss. Das FTP-Protokoll verwendet dabei einen Port für die Kontrollverbindung, die die Befehle und Statusinformationen übermittelt sowie einen dynamischen Port für die Datenverbindung.

Das FTP-Protokoll verwendet zwei unterschiedliche Betriebsmodi für die Datenübertragung, die beide vom IIS unterstützt werden:

- **Port-Methode**
  Wird die *Port-Methode* verwendet, baut der Server die Datenverbindung bei Bedarf zum Client auf. Dieses kann zu Problemen bei der Verwendung von Firewalls führen, die das Aufbauen einer Internetverbindung zum Client meistens verhindern soll. Das FTP-Protokoll enthält dafür eine passive Methode.
- **Passive Methode**
  Wird diese Methode zur Datenübertragung verwendet, baut der Client die benötigte Datenverbindung zum Server auf, der Server verhält sich *passiv*. Diese Methode kann für bestimmte Netzwerkkonfigurationen, die NAT (Network Address Translation) oder Firewalls verwenden, nötig sein.

Die Kontrollverbindung

Der FTP-Server wartet normalerweise auf TCP Port 21 darauf, eine Kontrollverbindung aufzubauen. Der Client verwendet dabei ein textbasiertes Protokoll, um sich zu authentifizieren, Verzeichnisse zu durchsuchen und um den Dateitransfer zum oder vom Server zu starten. Dabei wird die Authentifizierung unverschlüsselt in lesbarem Text übertragen, was das Abfangen von Passwörtern leider sehr erleichtert.

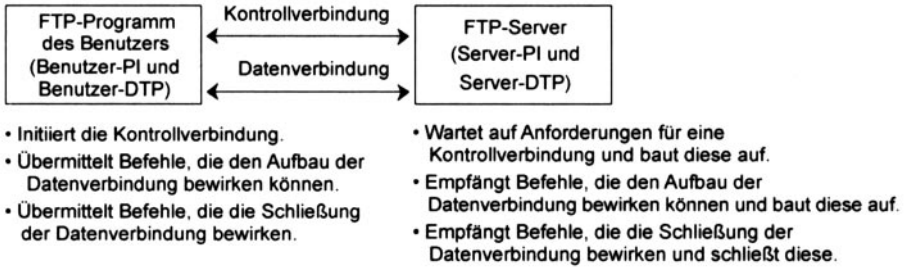

Abbildung 2-19 „Eine FTP-Sitzung zwischen einem Client und einem Server" [LEE00]

FTP Wiederaufnahme

Bricht eine Datenübertragung zusammen, bietet das FTP-Protokoll wenig, um den Datentransfer an der unterbrochenen Stelle wieder aufzunehmen. Der IIS 5.0 unterstützt die im FTP-Protokoll definierte Methode zur Übertragung der Dateien in einzelnen Blöcken. Viele FTP-Clients unterstützen inzwischen die Möglichkeit, den Datentransfer nach dem letzten übertragenen Block wieder aufzunehmen, wodurch Dateien nicht komplett neu übertragen werden müssen. Leider bietet das FTP-Protokoll keine Möglichkeit der Versionskontrolle der Dateien, wodurch der Server nicht feststellen kann, ob die Datei inzwischen verändert wurde.

WebDAV

Das *WebDAV-Protokoll* bietet die zweite Möglichkeit einen Dateiserver mit dem IIS bereitzustellen und ist in FRC 2518 definiert. Es ermöglicht die Verwendung des HTTP-Servers als Dateiserver, der mit einem geeigneten Client plattformunabhängig verwendet werden kann.

Das HTTP-Protokoll stellt dabei die HTTP-Anforderungen GET, PUT und DELETE zur Verfügung, womit bereits Dateien geschrieben und verändert werden können. Das WebDAV-Protokoll erweitert nun das HTTP-Protokoll um weitere Funktionen.
Die WebDAV-Erweiterung ermöglicht die Versionsverwaltung auf dem Webserver, so dass mehrere Benutzer den Server verwenden können und kein Benutzer aktuellere Dokumente eines anderen Benutzers aus Versehen überschreibt. Außerdem können Dateien auf dem Server gesperrt werden, damit andere Benutzer erkennen können, dass diese Datei auf dem Server gerade verwendet wird. Nach der Verwendung wird die Datei für andere Benutzer wieder freigegeben.
Dieses noch recht neue Protokoll könnte das vorhandene Protokoll zur Übertragung von Daten im Internet, das FTP Protokoll, ablösen. Obwohl es selbst keine sichere Authentifizierung und Verschlüsselung bei der Übertragung der Daten liefert, kann es mit vorhandenen Protokollen, wie SSL oder Kerberos, kombiniert werden. Dadurch wäre eine sichere Übertragung der Daten und eine sichere Authentifizierung der Benutzer möglich; dies sind die größten Probleme beim FTP-Protokoll.

Empfangen und Weiterleiten von E-Mails (SMTP Protokoll)

Eine weitere Funktion des IIS ist der eingebaute SMTP (Simple Mail Transfer Protocol) Server. Der SMTP-Server erlaubt die Entgegennahme von E-Mails und versucht, diese in lokale Postfächer zu verteilen. Gelingt ihm das nicht, versucht er andere SMTP-Server zu erreichen, die für die Mailempfänger verantwortlich sind und leitet die E-Mails an diese weiter (Relay).
Dabei ist der SMTP-Server kein vollwertiger Mail-Server, es fehlt z.B. die Möglichkeit, E-Mails abzuholen oder Benutzerkonten einzurichten. Vielmehr soll der SMTP-Server Möglichkeiten bieten, E-Mails zu versenden (z.B. von einer Website aus).
Der SMTP-Server kann natürlich auch von vollwertigen Mailservern verwendet werden. Der Microsoft Exchange Server verwendet bspw. diesen Dienst.

Senden und Empfangen von E-Mails

Der SMTP-Server kann von anderen Programmen zum Versenden und Empfangen von E-Mails nach [RFC0821] und [RFC0822] verwendet werden.
Dafür richtet der SMTP-Server fünf Verzeichnisse ein, in denen die entsprechenden E-Mails gespeichert werden:

SortTemp	Dies ist ein temporäres Verzeichnis für den SMTP Server.
BadMail	In diesem Verzeichnis landen E-Mails, die nicht zugestellt werden können.
Drop	Alle eingehenden E-Mails werden hier gespeichert.
Pickup	Textdateien, die in diesem Ordner gespeichert werden, werden vom SMTP-Server automatisch ausgeliefert.
Queue	Dies sind die E-Mails, die zur Zeit auf Zustellung warten.

Der SMTP-Server wartet normalerweise darauf, dass ein SMTP-Client eine Verbindung an TCP Port 25 aufbaut und SMTP-Befehle sendet. Diese beinhalten dann verschiedene Informationen und die E-Mail. Danach wird die TCP-Verbindung abgebaut.

SMTP Server und virtuelle Server

Obwohl nur ein SMTP Server vorhanden ist, können mehrere *virtuelle Server* eingerichtet werden. Diese können unterschiedliche Domänen verarbeiten und mit unterschiedlichen IP Adressen konfiguriert werden.
Für den SMTP-Server und alle virtuellen Server sind eine Reihe von Einstellungen vorzunehmen. So können die maximale Verbindungsanzahl, die IP-Adresse und die Port-Nummer geändert werden, die Protokollierung aktiviert und Einschränkungen für die Benutzung des SMTP-Servers vorgenommen werden.

Das SMTP Protokoll

Das *Simple Mail Transfer Protocol* wird in [RFC0821] definiert und beschreibt ein Client-Server Protokoll zur Übertragung von E-Mails. Das Mailprogramm baut dafür eine Verbindung zum SMTP-Server auf und überträgt die Mail mit Informationen über den Absender und den Adressaten in einer Verbindung, die durch Textkommandos gesteuert wird.
Ist die Übertragung der E-Mail abgeschlossen, wird der SMTP-Server versuchen, diese an den Empfänger weiterzuleiten.
Die Informationen, die während der Verbindung übertragen werden, beschränken sich im wesentlichen auf den Text der E-Mail, den Absender und die oder den Empfänger. Eine Authentifizierung des Clients findet normalerweise nur über die Absenderadresse statt und wird nicht überprüft. Die Daten der E-Mail werden in Klartext übertragen und können während der Übertragung abgehört werden.

Sicherheit

Obwohl das SMTP Protokoll keine Authentifizierung bietet, wurde der SMTP-Server von Windows 2000 um diese Funktionen erweitert. So können Nachrichten bei der Übertragung verschlüsselt werden und Clients, die E-Mails senden wollen, können zu einer gültigen Authentifizierung gezwungen werden. Diese Methoden müssen natürlich von der Gegenstelle unterstützt werden, sind in einem Intranet aber hilfreich.
Diese Funktionen können verwendet werden, um einen SMTP-Server, der Zugang zum Internet hat, davor zu schützen, als E-Mail-Server für Werbung eingesetzt zu werden.

Der Newsgroups Server

Der IIS beinhaltet einen vollständigen *Newsgroup-Server*, der zur Erstellung und Verwaltung von internen oder öffentlichen *Diskussionsforen* verwendet werden kann und für die Übertragung das *Network News Transfer Protocol (NNTP)* benutzt.
Wie der SMTP-Server, kann auch der NNTP-Server um Funktionen, wie sichere Übertragung der Daten und Authentifizierung, erweitert werden, wobei die Clients diese Erweiterungen unterstützen müssen.
Der NNTP-Server verwendet eine lokale oder entfernte Ordnerstruktur zum Speichern der Beiträge, wofür bei der Installation zwei Ordner ausgewählt werden. Der erste Ordner beinhaltet interne Dateien für den Newsserver und der zweite Ordner die Verzeichnisstruktur und Dateien für die Newsgroups.

Es können mehrere Newsgroups und auch mehrere virtuelle NNTP-Server erstellt werden, die wie die virtuellen SMTP-Server eigene IP-Adressen oder Portnummern (normalerweise 119) zugeordnet bekommen.

Newsgroups

Ein Newsserver verwaltet eine Reihe von Foren, die *Newsgroups* genannt werden und Nachrichten enthalten können. Ein Benutzer kann diese Nachrichten herunterladen oder eigene in eine Newsgroup posten, die dann wiederum von anderen Benutzern gelesen werden können. Eine Nachricht besteht aus einem Nachrichtenheader und einem Nachrichtentext, so dass der Benutzer nicht die gesamte Nachricht herunterladen muss, sondern dies anhand des Headers entscheiden kann.
Die Nachrichten bestehen aus reinem Text und können Anhänge enthalten. Ihr Format wird in [RFC0850] definiert und entspricht dem *USENET-Format*.

Das Network News Transfer Protocol (NNTP)

Das NNTP-Protokoll wird in [RFC0977] definiert und verwendet textbasierte Befehle für die Kommunikation zwischen Server und Client, die den Befehlen des SMTP-Protokolls ähnlich sind. Der Client schickt einen Befehl zum Server, mit dem bspw. eine Nachricht oder eine Nachrichtenliste heruntergeladen werden soll, der Server beantwortet die Anforderung mit einem Statuscode und wenn möglich mit den angeforderten Daten. Texte werden wie im SMTP-Protokoll durch einen Punkt „.“ auf einer einzelnen Textzeile beendet.

Sicherheit

Der NNTP-Server in Windows 2000 besitzt ähnliche Sicherheitsfunktionen wie der SMTP-Server. Daten können durch TLS während der Übertragung verschlüsselt werden und Benutzer können gezwungen werden, sich zu authentifizieren. Dadurch kann ein interner Newsgroup-Server vor dem Zugriff von außen geschützt werden.

Drucken mit dem IIS, das Internet Print Protocol (IPP)

Eine weitere Funktion des IIS 5.0 ist die Unterstützung des *IPP-Protokolls*, mit dem Clients über das HTTP-Protokoll auf Drucker im Netzwerk zugreifen können. Der Ablauf eines solchen Druckjobs sieht folgendermaßen aus. Der Client, dabei kann es sich um einen Browser, einen Druckertreiber mit IPP-Unterstützung oder ein anderes Programm handeln, sendet seinen Druckauftrag in Form einer HTTP 1.1 Anforderung an eine bestimmte URL. Diese Anforderung enthält den IPP Druckauftrag und die Druckdaten.
Der Drucker wird dazu im Active Directory angelegt und enthält Informationen über die Leistungsfähigkeit des *Druckobjekts*. Das Druckobjekt ist allerdings kein physikalischer Drucker, sondern nur ein logisches Objekt im AD. Nach dem Empfang des Druckauftrags wird dieser nun vom Druckobjekt im Active Directory an einen wirklichen Drucker weitergeleitet. Dabei kann ein Druckobjekt mehrere wirkliche Drucker verwenden, um seine Leistungsfähigkeit zu erhöhen. Als Druckziel könnte allerdings auch eine Software in Frage kommen, die aus dem Druckauftrag bspw. ein PDF erzeugt.

Dabei muss der wirkliche Drucker oder die Software, die als Druckziel auftritt, keine IPP-Fähigkeiten besitzen, dafür sorgt das Druckobjekt. Ist der Drucker in der Lage das IPP-Protokoll zu verarbeiten, kann das Druckobjekt die Anfrage aber auch direkt an den Drucker weiterleiten. Das Druckobjekt dient dann lediglich dazu, den Drucker im Verzeichnisdienst erscheinen zu lassen.
Der IIS übernimmt in diesem Zusammenhang die Übertragung der Daten vom und zum Client. Da die Anforderungen mit Hilfe des HTTP-Protokolls an den Server geschickt werden, empfängt der IIS diese Anforderung, leitet diese an die ISAPI-Anwendung (siehe Webserveranwendungen) für IPP-Aufträge weiter und schickt eine Antwort an den Client.

Abbildung 2-20 „Gefächerte IPP-Druckverarbeitung" [LEE00]

Das Internet Print Protocol (IPP)

Das IPP Protokoll ist in den RFCs [RFC2565] und [RFC2566] definiert und ist aus zwei Schichten aufgebaut. Die erste Schicht ist die *Transportschicht*, die HTTP-Anforderungen beschreibt. Die zweite Schicht, die *Verarbeitungsschicht*, behandelt den in den HTTP-Anforderungen und -Antworten eingebetteten Nachrichteninhalt.
Jede Anforderung oder Antwort enthält eine Reihe von Attributen, die Auskunft über den Status der Druckanforderung oder das Leistungsspektrum des Druckerobjekts geben.
Diese Attribute lassen sich in vier Kategorien einordnen:

- **Druckerattribute**
  Diese enthalten Informationen über den Drucker (das Druckerobjekt) oder über die Eigenschaften von Druckjobvorlagen, die das Druckerobjekt verarbeiten kann.
- **Druckjobattribute**
  Diese Attribute enthalten Informationen über Druckjobs. Dies können der Status oder andere Eigenschaften eines Druckjobs sein.
- **Verarbeitungsattribute**
  Hierbei handelt es sich um Attribute, die Informationen über Transaktionen enthalten und zwischen dem Client und dem Druckerobjekt stattfinden.
- **Unbekannte Attribute**
  Da das IPP Protokoll erweiterbar ist, ist es möglich, dass ein Druckerobjekt einige Attribute nicht versteht. Das Druckerobjekt wird diese Attribute dann in eine Meldung verpacken und an den Client zurücksenden, damit dieser die Attribute nicht weiter verwendet.

Der Client schickt eine Druckanforderung an den IPP-Server (das Druckerobjekt). Diese Anforderung enthält Verarbeitungsattribute, Objektattribute und die Dokumentdaten. Der Client sendet diese Anforderung an die URL des Druckobjekts. Jede Anforderung wird mit einer Antwort bestätigt, die eine Statusmeldung beinhaltet und weitere Attribute, die Informationen über den Status

und das evtl. angelege Druckjobobjekt enthalten. Dieses erhält eine eigene URL und kann evtl. weitere Dokumente aufnehmen, die nacheinander abgearbeitet werden.
Damit der Client die Antworten vom Server zuordnen kann, erhält jede Anforderung eine *Vorgangs-ID*, eine *Versionsnummer* und eine *Anforderungs-ID*. Die Antwort vom Server enthält dann ebenfalls eine Versionsnummer, einen Statuscode und die vom Client gesendete Anforderungs-ID.

Sicherheit

Durch die Verwendung des HTTP-Protokolls als Transportprotokoll und die Verarbeitung der Anforderungen durch den IIS gibt es die gleichen Sicherheitsfunktionen, wie bei einer normalen Website. Die Anforderung kann anonym oder durch einen authentifizierten Benutzer erfolgen und über TLS/SSL verschlüsselt werden. Sollte der Server an das Internet angebunden sein, sind also unbedingt Sicherheitsmaßnahmen zu treffen, damit nicht jeder die internen Drucker verwenden kann.

Technische Details

Der IIS 5.0 gehört zu den *Betriebssystemdiensten*, d.h. es muss kein Programm von einem Benutzer gestartet werden, sondern der Dienst wird automatisch beim Start von Windows 2000 aktiviert, also bevor sich ein Anwender am Server interaktiv anmeldet. Das hat den Vorteil, dass im Falle eines Serverneustarts der IIS wieder einsatzbereit ist, hat aber auch den entscheidenden Nachteil, dass der Dienst unbeobachtet abläuft und im Sicherheitskontext des Systems ausgeführt wird.
Eine Erläuterung der Gefahren in Bezug auf die Serversicherheit findet in Kapitel 4.2.6 statt.
Damit allerdings nicht alle Internetbesucher im Sicherheitskontext des Systems auf dem Server erscheinen, nimmt der IIS für den anonymen Internetuser die Identität des Internetgastkontos (IUSR_<computername>), bzw. für einen authentifizierten Benutzer dessen Identität an.
Welches Benutzerkonto für den *Identitätswechsel* verwendet wird, sowie die Einstellungen für den Dienst, also, ob er gestartet wird und in welchem Sicherheitskontext er läuft, kann allerdings jederzeit geändert werden.

Active Directory und das Active Directory Service Interface (ADSI)

Der IIS speichert die Daten seiner Konfiguration, wenn möglich, im Active Directory. Der Speicherbereich, der auch *Metabasis* genannt wird, enthält alle Einstellungen des IIS, alle Einstellungen der Websites und die Konfiguration der FTP-Server.
Die Metabasis kann, wie andere Bereiche des Active Directorys, über das *Active Directory Service Interface (ADSI)* bearbeitet werden. Dadurch haben Script- und Programmiersprachen Zugriff auf die Konfiguration des IIS und können diese auslesen und verändern. Die im Folgenden erläuterte Remoteverwaltung des IIS verwendet bspw. diese Schnittstelle zur IIS-Konfiguration.

Prozesse

Um die Stabilität des IIS zu erhöhen, können einzelne Aufgaben auf mehrere *Prozesse* aufgeteilt werden. Dies betrifft hauptsächlich den Webserver, dieser erlaubt die Aufteilung von Basisverzeichnissen oder virtuellen Verzeichnissen auf einzelne Prozesse, die unterschiedliche Speicherbereiche belegen. Stürzt ein Prozess, z.B. eine Website, ab, so werden andere Prozesse nicht beeinträchtigt.

Diese Prozesse können nun zur Erhöhung der Stabilität der anderen Prozesse auf dem Server überwacht und eingeschränkt werden. Nimmt ein Prozess z.B. zu viel CPU-Leistung in Anspruch, kann er beendet oder neu gestartet werden. Auch die Einschränkung der verwendeten Netzwerkbandbreite ist möglich. Dadurch soll erreicht werden, dass ein „hängender" Prozess die anderen Prozesse nicht negativ beeinflussen kann.
Dieses muss jedoch manuell eingerichtet werden, da die Standardkonfiguration alle Threads in dem IIS-Prozess startet. Stürzt einer dieser Threads (z.B. die oben erwähnte Website) ab, so wird auch der IIS Dienst im ungünstigen Fall komplett abstürzen und muss manuell oder automatisch neu gestartet werden.

Webserveranwendungen

Obwohl die meisten Webangebote statische Inhalte enthalten, gibt es zahlreiche Anwendungsgebiete bei denen die Inhalte der Internetseiten z.B. aus Datenbanken generiert werden. Für solche Webserveranwendung bietet der IIS Schnittstellen, die von Webentwicklern benutzt werden können.

Anwendungserstellung

Damit eine Website Programme, Scriptsprachen oder andere dynamischen Elemente verwenden kann, wird eine *Anwendung* erstellt. Diese wird dann als Ausgangspunkt für alle Programme, Scripte, etc. verwendet. Verschiedene Anwendungen laufen voneinander getrennt ab, so dass sie sich nicht gegenseitig stören können. Es ist sinnvoll mehreren Websites auf einem Server unterschiedliche Anwendungen zuzuordnen, damit z.B. Artikel von einer Website nicht im Warenkorb einer anderen Website auf dem gleichen Server auftauchen.
Generell wird für jede neue Website eine neue Anwendung erstellt, es können aber auch innerhalb einer Website mehrere Anwendungen, z.B. für unterschiedliche virtuelle Verzeichnisse, existieren.
Eine Anwendung kann im IIS Prozess, in einem zusammengefassten Prozess oder in einem eigenen Prozess laufen. Die Trennung der Anwendungen in verschiedene Prozesse mag sinnvoll erscheinen, ist allerdings auch mit einem erhöhten Speicherbedarf verbunden. Unabhängig von anderen Anwendungen und dem IIS können diese entladen (also zurückgesetzt) werden, ohne dass der Webserver dafür angehalten werden muss.
Jede Anwendung besitzt eine Sammlung von Programmen, Scripten und anderen Komponenten, die sich von anderen Anwendungen unterscheiden kann. Für die Einbindung von Programmen bietet der IIS folgende Schnittstellen:

Das Common Gateway Interface (CGI)

Das *Common Gateway Interface (CGI)* ist einer der ältesten Schnittstelle zwischen einem Webserver und einem Programm oder einem Script und ein plattformübergreifender Standard. Dabei wird eine Anfrage durch eine URL an ein Programm oder Script gestellt, das dann vom IIS aufgerufen wird, die Parameter der Anfrage übertragen bekommt und eine Antwort, meist in Form einer Internetseite, liefert, die der IIS dann zurück an den Client sendet. Diese Programme oder Scripte können dabei in einer beliebigen Programmiersprache geschrieben sein, solange dessen Entwick-

lungswerkzeuge die Erstellung von CGI gestatten, bzw. ein entsprechender Scriptinterpreter vorhanden ist.
Der größte Nachteil dieser Schnittstelle ist die geringe Performance durch den Programmaufruf und die Notwendigkeit, bei jeder Änderung der Software, diese neu kompilieren zu müssen.

ISAPI

Die ISAPI ist eine API, um COM-Objekte zu erstellen, die eine Schnittstelle besitzen, über die der IIS mit ihnen kommunizieren kann. Diese Weiterentwicklung der CGI-Schnittstelle erlaubt die direkte Verwendung von COM-Objekten durch den IIS. Der Hauptgrund der Verwendung von *ISAPI-Komponenten* liegt in der wesentlich höheren Performance gegenüber der CGI-Schnittstelle und der Möglichkeit, umfangreichere Systemdienste zu verwenden. Allerdings müssen auch diese Komponenten bei einer Änderung neu kompiliert werden.
Nach der Installation des IIS sind schon eine ganze Reihe von ISAPI-Anwendungen enthalten, die durch Dateinamensendungen den einzelnen Komponenten zugeordnet sind. Diese stellen z.B. Verbindungen zum Indexdienst oder zum WebDAV-Dienst her. Beide Dienste sind durch eine ISAPI-Schnittstelle mit dem IIS verbunden.

Die Active Server Pages (ASP) Anwendung

Die *ASP-Anwendung*, die ausführlich im nächsten Kapitel beschrieben wird, bietet eine weitere Möglichkeit, Anwendungen zu erstellen.
ASP Anwendungen werden mit verschiedenen *Scriptsprachen* programmiert, die in vorhandene Internetseiten integriert werden können. Diese werden nicht kompiliert und bei einer Änderung direkt bearbeitet, wodurch die ASP-Anwendungen flexibler sind als die bereits genannten Komponenten.
Die Scriptsprachen können erweitert werden, Microsoft liefert Interpreter für VB Script, eine Art Visual Basic und für JScript, eine Art JavaScript, aus. Diese können durch weitere, z.B. PerlScript, ergänzt werden. Innerhalb der Scriptsprache können außerdem andere COM-Objekte aufgerufen und verwendet werden, wodurch eine Anbindung an das Active Directory oder an Datenbanken möglich wird.

Zusammenfassung

Der IIS ist mehr als nur ein Webserver und sollte daher nach einer Installation auch so behandelt werden. Kennt sich ein Administrator nicht mit den übrigen Funktionen aus, kann er schnell mit einem Mausklick zuviel die gesamte Festplatte über das Internet freigeben. Auch andere Funktionen, wie das Weiterleiten von E-Mails, werden gerne ausgenutzt und nach Servern, die solche Weiterleitungen erlauben, wird regelrecht im Internet gesucht.
Der Einsatz von Anwendungen, Scriptsprachen und Programmen erweitert die Funktionalität des IIS, ist aber ebenfalls gefährlich, wenn sie falsch konfiguriert wird.

2.2.7 Active Server Pages (ASP) und ASP.net (ASP+)

Die im letzten Kapitel vorgestellten *Active Server Pages* bieten in Verbindung mit dem IIS die Möglichkeit, Scriptsprachen direkt in Internetseiten zu verwenden. Wird eine solche Internetseite über den Webserver im IIS aufgerufen, werden die Scripte verarbeitet und können bspw. Daten in Datenbanken verändern oder auslesen oder Dateien im Dateisystem verwenden.

Die im IIS verwendete Version der Active Server Pages (Version 3.0) enthält einige neue Funktionen. Nach der Installation des Betriebssystems können VBScript und JScript als Scriptsprachen in Internetdokumenten verwendet werden, weitere können durch zusätzliche Module von Drittanbietern hinzugefügt werden.
Die enge Verbindung des IIS mit anderen Systemkomponenten und die Möglichkeit, in ASP auf Systembestandteile, wie das Dateisystem, Datenbanken oder das Active Directory, zuzugreifen, ermöglichen eine große Vielfalt an unterschiedlichen Funktionen, die mit ASP erledigt werden können. Da jedoch meistens der Webserver aus dem öffentlichen Netz zugänglich ist, ist die Vielfalt an möglichen Gefahren, die daraus entstehen, ebenso groß. Diese werden in Kapitel 4 beschrieben und resultieren meistens aus fehlerhafter Programmierung von Webapplikationen.

Funktionsweise von ASP

ASP ist im IIS als ISAPI-Anwendung realisiert. Eine DLL (asp.dll) wird mit verschiedenen Dateinamensendungen („.asp", „.asa" etc.) verbunden und wenn der IIS eine Anforderung für eine solche Datei erhält, wird diese an dieDLL weitergeleitet. Ohne Änderungen der Konfiguration des IIS wird für jede neue Website eine Anwendung erstellt, die auch die ASP-Anwendung enthält. D.h., dass jede neue Website die ASP-Anwendung verwenden kann, auch wenn keine entsprechenden Dateien vorhanden sind.
Die Realisierung von ASP durch eine ISAPI-Anwendung erlaubt es, die eigentliche asp.dll entweder im gleichen Prozess mit dem IIS oder in einem eigenen Prozess laufen zu lassen. Neu seit Version 5.0 des IIS ist die Möglichkeit, alle ISAPI-Anwendungen in einem eigenen Prozess laufen zu lassen, der vom IIS getrennt ist.
Die asp.dll analysiert das angeforderte Dokument auf Vorhandensein von Scriptblöcken, wertet diese aus und übergibt das resultierende Dokument an den Besucher. Dabei werden alle Scriptblöcke und Scripttags aus dem Dokument entfernt, so dass der Besucher diese nicht zu sehen bekommt. Eine einfache ASP-Internetseite kann folgendermaßen aussehen:

```
<HTML>
<HEAD>
<TITLE>Eine Beispielseite</TITLE>
</HEAD>
<BODY>
<%
      response.write "Dieser Text wird durch den ASP-Code erzeugt."
%>
</BODY>
</HTML>
```

Der Browser des Besuchers bekommt dann folgendes Dokument vom Server:

```
<HTML>
<HEAD>
<TITLE>Eine Beispielseite</TITLE>
</HEAD>
<BODY>
Dieser Text wird durch den ASP-Code erzeugt.
</BODY>
</HTML>
```

Die Scriptblöcke werden in den <% .. %> Tags eingeschlossen und durch die asp.dll verarbeitet. Der Befehl ‚response.write' schreibt den angegeben Text in das HTML Dokument, wobei das eigentliche Script aus dem Dokument entfernt wird. Für die Integration des Scriptblocks kann noch eine weitere Methode verwendet werden, die mit XML/XHTML[25] verträglich ist:

```
[...]
<BODY>
<SCRIPT LANGUAGE="VBScript" RUNAT="server">
      response.write "Dieser Text wird durch den ASP-Code erzeugt."
</SCRIPT>
</BODY>
[...]
```

Diese Methode ist mit der Einbindung von Scriptblöcken in Internetseiten identisch, die asp.dll erkennt das „runat"-Attribut und verarbeitet das Script. Auch bei dieser Methode verschwindet der Scriptcode für den Benutzer.

Erweiterbarkeit durch COM Komponenten

Obwohl die verwendeten Scriptsprachen VBScript und JScript schon eine ganze Reihe von Funktionalitäten bieten, wird erst durch die Möglichkeit der Einbindung von COM-Objekten eine sinnvolle Anwendung möglich. Solche COM-Objekte können entweder vorhandene Komponenten, die Verbindungen zu Datenbanken (ADO Objekt), zum Dateisystem (Filesystem Objekt), zu XML Dokumenten (XML Parser) oder zum Active Directory (ADSI Schnittstelle) ermöglichen oder selbst entwickelte Komponenten sein, die eigens entworfen worden sind oder von Drittanbietern inzwischen für viele Aufgaben fertig angeboten werden.

Zugriffsrechte

Die ISAPI-Anwendungen werden im Sicherheitskontext des IIS ausgeführt, der für den jeweiligen Internetbesucher entweder die Identität des Internetgastkontos (IUSR_<Computername>) oder die des authentifizierten Benutzers annimmt. Dadurch werden alle Aktionen, die innerhalb der

25 XHTML ist eine HTML-Variante, die zu XML kompatibel ist.

ASP-Anwendung ablaufen, mit den Benutzerrechten des jeweiligen Internetbesuchers durchgeführt. Sollen weitere Benutzerrechte hinzugefügt werden, so kann dies durch die Benutzerkonten erfolgen, die Ausweitung von Benutzerrechten des Internetgastkontos ist allerdings mit Gefahren verbunden.

ASP-Anwendungen

Die Verwendung von ASP in einer einzelnen Internetseite wird nur für wenige Anwendungen ausreichen. Die Erstellung einer Anwendung im IIS legt den Rahmen fest, inwieweit Dokumente in der Verzeichnisstruktur des Webservers zu einer ASP-Anwendung zusammen gefasst werden. Alle Dateien in Unterverzeichnissen gehören zur gleichen ASP-Anwendung, Dateien, die in der Verzeichnishierarchie über dem Anwendungsbasisverzeichnis liegen, gehören nicht mehr dazu. Innerhalb einer Anwendung können Objekte und Informationen über mehrere HTTP-Anforderungen verwendet werden. ASP bietet dazu das ‚Appclication'-Objekt, das in jeder ASP-Seite wiederverwendet werden kann und alle gespeicherten Informationen oder Objekte solange behält, bis der Webserver oder die Anwendung neu gestartet wird.

Benutzersitzungen

Obwohl das HTTP-Protokoll keine eigene Verwaltung für Benutzersitzungen enthält und alle Anforderungen ohne Bezug auf die Benutzersitzung abgearbeitet werden, erlaubt ASP die Verwendung von Objekten und Informationen zwischen mehreren HTTP-Anforderungen von einem individuellen Besucher, solange diese in einer ASP-Anwendung enthalten sind.
Diese Benutzersitzung wird durch die Verwendung eines *Cookies* [26]ermöglicht, das der Benutzer bei der ersten Anforderung an eine ASP-Seite enthält. Dieses Cookie enthält die *Sitzungs-ID* der Sitzung und wird von der asp.dll verwaltet.
Das ‚Session'-Objekt speichert Informationen und Objekte, die nur von einem Besucher innerhalb einer Anwendung verwendet werden können. Diese Funktion wird häufig für Warenkörbe verwendet. Ruft der Besucher innerhalb einer einstellbaren Zeit keine neuen ASP-Seiten innerhalb der Anwendung auf, wird die Sitzung gelöscht und der verwendete Speicher wieder freigegeben.
Lässt der Besucher die Verwendung von Cookies nicht zu, funktionieren die Sitzungen nicht und ASP wird mit jeder Seite erneut versuchen, ein Sitzungscookie zu erstellen. Diese Funktion kann für einzelne ASP-Seiten oder für eine gesamte Anwendung deaktiviert werden. Sollte die Anwendung keine Sitzungen verwenden, empfiehlt sich die Deaktivierung aus Gründen der Performance.

Die global.asa Datei

Sowohl das ‚Application'-Objekt, als auch das ‚Session'-Objekt bieten eine Reihe von Standardmethoden. So können für beide Objekte eine ‚Start'- und ‚End'-Methode definiert werden, die ausgeführt werden, wenn eine Anwendung oder eine Sitzung gestartet bzw. wieder gelöscht wird. Damit können z.B. für einen neuen Besucher Standardeinstellungen einer Sitzung festgelegt und bei Sitzungsende wieder gelöscht werden.

---

26 Ein Cookie ist ein kurzer Text, der von einer Website im Browser des Besuchers gespeichert und bei Bedarf wieder abgerufen werden kann.

Diese Methoden werden in einer speziellen Datei definiert, die den Namen *‚global.asa'* trägt und sich im Basisverzeichnis einer Anwendung befinden muss. Es können also für verschiedene Anwendungen, die alle ein anderes Basisverzeichnis haben, verschiedene ‚global.asa'-Dateien angelegt werden.

Transaktionen und COM+ Unterstützung

Die Unterstützung der COM+-Architektur durch ASP erlaubt die Verwendung von Transaktionen des Microsoft Transaction Servers. Eine Transaktion zeichnet alle Aktionen auf und kann diese bei einem Fehler wieder rückgängig machen. Die Verwendung dieser Funktion setzt allerdings transaktionsfähige Komponenten voraus.

ASP.net (ASP+)

Nach der Einführung der *.net Kampagne* wurde die gerade in Entwicklung befindliche Erweiterung *ASP+* in *ASP.net* umbenannt. Diese steht momentan allerdings nur als Betaversion zur Verfügung und ist daher noch nicht sicherheitsrelevant.
In ASP sind die HTML-Komponenten von den ASP-Funktionen getrennt. Ein HTML-Designer kann z.B. eine Formularseite entwerfen, die von einem Besucher ausgefüllt werden soll. Diese Daten werden dann an eine ASP-Seite geschickt, die die Informationen auswertet und bspw. in eine Datenbank schreibt. ASP.net erlaubt die direkte Verbindung zwischen dem HTML-Code und dem ASP-Script. Der Entwickler erstellt ein Formular und setzt dort Formularfelder ein, die mit einer Datenbank verbunden werden. ASP+ erstellt den entsprechenden ASP-Code und die HTML-Elemente, um die Funktion für den Besucher zu realisieren.
ASP+ soll dabei zwei Aufgaben erledigen: Zum einen wird der ASP- bzw. ASP+-Code sehr viel leserlicher, als die bisherige Verwendung von ASP-Scriptblöcken und außerdem wird die Erstellung solcher Funktionen erleichtert.
Allerdings wird dies nicht die einzige Funktion von ASP+ sein. Hinzu kommen neue Programmiersprachen, wie Visual Basic, C++ und C#, die in ASP verwendet werden können.
Da sich die gesamte .net Initiative noch in der Beta-Phase befindet, werden sich wohl noch einige Veränderungen ergeben.

Zusammenfassung

ASP bietet einem Webentwickler die Möglichkeit, dynamische Funktionen in eine Website auf einem Windows 2000 Server zu integrieren. Die Funktionen sind sehr umfangreich und können durch weitere Komponenten erweitert werden. Die Kombination von ASP mit anderen Diensten, wie z.B. Datenbanken, XML und das Active Directory, zeigt, wie weit der IIS und seine Funktionen mit dem restlichen Betriebssystem verbunden sind.

2.2.8 Terminaldienste

Die in Windows 2000 integrierten *Terminaldienste* erlauben neben der entfernten Verwaltung eines Servers auch die Verwendung von Windows 2000 als Client/Server basiertes Anwendungssystem.
Ein Terminal ist eine ferngesteuerte Version einer direkten Anmeldung an einem Terminalserver. Die Mausbewegungen und Tastaturanschläge werden an den Terminalserver übertragen und der Terminalclient empfängt die grafische Darstellung der Benutzerschnittstelle (im Grunde genom-

men das Monitorbild). Die Terminaldienste ähneln daher dem *Telnetserver*, der allerdings nur die Verwendung einer Textkonsole ermöglicht oder anderen Terminalprogrammen, wie bspw. unter UNIX-Betriebssystemen. Ein Windows 2000 Terminalserver kennt zwei Betriebsmodi:

Anwendungsservermodus

Der *Anwendungsservermodus* wird von Clients verwendet, die nicht auf ihren lokalen Clientsystemen arbeiten, sondern die Leistungsfähigkeit und die Ressourcen des Servers verwenden. Dies hat entsprechende Vorteile, da die Clientsysteme wesentlich geringere Hardwareanforderungen erfüllen müssen, der Server dagegen muss entsprechend mehr Leistung besitzen. Ein weiterer Vorteil ist die einfachere Verwaltung der Clients und des Netzwerks, da Dateien und Programme auf dem Server gespeichert werden, bzw. dort ablaufen und dort auch die Verarbeitung der Daten erfolgt. Daten können leichter zentral am Server gesichert werden und Programme werden zentral installiert und konfiguriert. Die Überwachung von Prozessen und Objekten kann ebenfalls zentral am Server erfolgen und erleichtert die gesamte Überwachung des Systems durch einen Administrator.

Remoteverwaltungsmodus

Dieser Betriebsmodus erlaubt die Anmeldung von max. zwei Terminalclients am Server und wird zur Administration des Server verwendet. Über den Terminalclient hat ein Administrator die Möglichkeit, alle Einstellungen am Server über die gewohnte grafische Benutzeroberfläche vorzunehmen und er hat Zugriff auf alle Administrationstools. Die Beschränkung auf zwei Terminalsitzungen erlaubt die Verwendung des *Remoteverwaltungsmodus* ohne zusätzliche Clientlizenzen für Terminaldienste.

Übertragung

Der Terminaldienst verwendet für die Übertragung der Daten das *Remote Desktop Protocol (RDP)*, dass auch schon für den Windows NT 4.0 Terminalserver verwendet wurde. Das Protokoll verwendet TCP/IP als Transportprotokoll und kann auch durch IP-Tunnel, oder über WAN-Verbindungen verwendet werden. Es ist ein mehrkanalfähiges Protokoll, das separate Kanäle für die Übertragung von unterschiedlichen Geräten (Tastatur, serielle Geräte) verwendet und in der Lage, die Daten für die Übertragung zu verschlüsseln.
Die Protokoll verwendet dafür den Port 3389 und kann auch durch eine Firewall transportiert werden. Durch die Übertragung von Tastatur- und Mausaktionen und die Daten für die grafische Oberfläche, benötigt der Terminaldienst nur eine geringe Bandbreite und kann auch über WAN- oder ISDN-Verbindungen verwendet werden.

Terminaldienst-Client und Anmeldung

Terminalclients gibt es für unterschiedliche Windows-Betriebssysteme von Windows 9x bis zu Windows 2000 und als 16 Bit- bzw. als 32 Bit-Version. Auch für *WindowsCE* ist ein Terminalclient vorhanden, mit dem der Administrator seinen Server auch von unterwegs verwalten kann.
Der Benutzer meldet sich mit seinem Benutzerkonto oder einem vorgegebenen Konto an den Terminalserver an und verwendet die Sicherheitseinstellungen seines Benutzerkontos, wobei die Anmeldung einzelnen Benutzern oder Gruppen verboten oder erlaubt werden kann.
Der Windows 2000 Terminalserver kann außerdem in einen mit NT 4.0 kompatiblen Modus ver-

setzt werden. Dann kann der Terminalserver auch NT 4.0 kompatible Terminaldienste verwenden, aus Sicherheitsgründen sollte allerdings der Windows 2000 kompatible Modus verwendet werden. Unter Umständen funktionieren einige ältere Anwendungen, die für den Terminalserver von NT 4.0 entwickelt wurden, allerdings nicht mit dieser Einstellung.

Terminalsitzung

Wird eine Verbindung zu einem Terminalserver aufgebaut, dann erstellt der Terminalserver für diese Verbindung eine Terminalsitzung. Die Terminaldiensteverwaltung listet diese Sitzungen auf, und Administratoren bekommen darüber einen Überblick, wer sich gerade am Server angemeldet hat. Neben dieser Clientsitzung, die eine aktive oder inaktive Verbindung vom einem Client darstellt, existieren noch drei weitere Sitzungstypen. Die *Listener-Sitzung* wartet auf neue RDP-Clients und erstellt auf Anforderung des Clients eine neue Clientsitzung. Es wird pro *Verbindungstyp* eine Listener-Sitzung erstellt.
Die *Konsolensitzung*, die ebenfalls automatisch erzeugt wird, beschreibt die wirkliche Tastatur, Maus und den Monitor des Terminalservers. Eine Anmeldung an der Konsolensitzung entspricht also dem tatsächlichen Anmelden am Server. Die *Leerlaufsitzung* wird automatisch erstellt und wird von der Listener-Sitzung in eine Clientsitzung umgewandelt. Sie existiert, damit der Anmeldevorgang schneller vonstatten geht.
Eine Sitzung bleibt normalerweise auch bestehen, wenn die Verbindung zwischen Client und Server unterbrochen wurde. Das bedeutet, dass auch die gestarteten Programme geöffnet bleiben und der Benutzer weiterhin am Server angemeldet ist. Er kann eine neue Verbindung zum Terminalserver aufbauen und seine alte Sitzung wieder übernehmen.
Damit unterbrochene Sitzungen nicht unnötige Ressourcen belegen, kann eine Sitzung, deren Verbindung unterbrochen wurde, nach einem Timeout beendet werden. Geschieht dies, werden allerdings auch alle Programme und Prozesse, die in dieser Sitzung gestartet wurden, beendet und es kann zu Datenverlust kommen. Gerade im Remoteverwaltungsmodus ist die Vergabe von Timeouts sinnvoll, da nur maximal zwei Sitzungen aufgebaut werden können. Wird nun die Verbindung unterbrochen, bleibt die Sitzung bestehen. Passiert das auch mit der zweiten Sitzung, kann sich der Administrator nicht mehr über einen Terminalclient am Server anmelden. Durch ein Timeout werden Sitzungen irgendwann wieder freigegeben.
Der Administrator kann Sitzungen zurücksetzen, wodurch die Sitzung geschlossen wird und alle Programme und Prozesse der Sitzung beendet werden. Er kann außerdem eine aktive Sitzung überwachen, wenn er die entsprechenden Rechte hat, und sich die momentane Sitzung, also das „Monitorbild“, ansehen. Der eigentliche Benutzer merkt dies nur, wenn ein Administrator aktiv in die Sitzung eingreift und selbst mit der Maus oder Tastatur Befehle übermittelt. Der Terminalserver kann so konfiguriert werden, dass der momentane Benutzer einer Überwachung zustimmen muss.

Verwendung von Geräten und temporäre Dateien

Der Benutzer kann für eine Terminalsitzung Geräte zuordnen. Während der Terminalsitzung verwenden die Programme, die auf dem Server laufen, die Geräte des Clients. So können z.B. die Audiogeräte zugeordnet werden, damit ein Warnton nicht aus den Serverlautsprechern ertönt, sondern direkt beim Benutzer zu hören ist. Folgende Geräte erlauben eine Zuordnung:

- Audiogeräte
- Zwischenablage
- Serielle Anschlüsse
- Laufwerke
- Parallele Anschlüsse
- Windows-Drucker

Die Einstellungen, welche Geräte zugeordnet werden, kann entweder durch den Administrator oder den Benutzer erfolgen, wobei der Administrator die Zuordnung von bestimmten Geräten verhindern kann.
Viele Programme erzeugen temporäre Dateien, die normalerweise auf der Festplatte gelagert werden. Damit verschiedene Sitzungen nicht gegenseitigen Zugriff auf die temporären Dateien haben, wird für jede Sitzung ein eigener Ordner für diese erstellt und der Inhalt des Ordners beim Beenden der Sitzung gelöscht. Beide Einstellungen lassen sich allerdings auch ändern.

Zusammenfassung

Die Terminaldienste ermöglichen einem Administrator die entfernte Verwaltung seines Servers. Außerdem kann der Terminaldienst auch als Client/Server System für Anwendungssysteme verwendet werden. Beide Möglichkeiten basieren auf der gleichen Methode, die grafische Benutzerschnittstelle sowie Maus- und Tastaturaktionen zwischen Server und Client zu übertragen.
Wie alle Systeme, die eine entfernte Verwaltung eines Server erlauben, muss auch bei dem Terminaldienst genau festgelegt werden, welcher Benutzer welche Rechte hat, damit sich nicht plötzlich jeder Benutzer am Server anmelden kann.

3 Verschiedene Angriffstaktiken

In diesem Kapitel wird auf verschiedene Angriffstaktiken eingegangen, die über Netzwerke oder durch direkten Zugriff zum Rechner erfolgen können. Man sollte bei der Bedrohung durch Angriffe eingrenzen, mit welchen Arten von Angriffen man rechnen muss. Ist ein Rechner beispielsweise nicht über ein Netzwerk mit der Außenwelt (Internet, etc.) verbunden, muss man nur lokale Sicherheitsmaßnahmen wie Kennwortrichtlinien und Benutzerkontenrichtlinien einsetzen. Ist das Netzwerk allerdings potenziellen Angriffen aus dem Internet oder durch Einwahlleitungen ausgesetzt, ist es wichtig möglichst viele Punkte abzusichern. Darunter fallen auch Maßnahmen wie Firewalls und die Deaktivierung unbenutzter Ports, wobei dem zweiten Punkt besondere Aufmerksamkeit gewidmet werden sollte, da er sehr entscheidend für die Sicherheit des Systems ist.

Angreifer gehen normalerweise nach diesem Schema vor:

- 1. *Footprinting:* Der Angreifer grenzt die Größe des Zielnetzwerks ein, indem er die von außen erreichbaren IP-Adressen ausfindig macht, DNS-Auflösung betreibt (dies wird dem Angreifer leicht gemacht, wenn DNS-Zonentransfers eingeschaltet sind) und ‚traceroutes' nutzt, um die Struktur des Eingangs in das Netzwerk zu analysieren.
- 2. *Scanning:* An dieser Stelle erkundet der Angreifer seine Angriffsmöglichkeiten. Mit Ping-Scans werden erreichbare Rechner gesucht und auf diesen dann durch Port-Scans nach offenen Ports gefahndet. Dieser Punkt ist entscheidend, da man anhand der offenen Ports eines Systems in Standardkonfiguration das Betriebssystem und seine Version nachvollziehen kann, was dem Angreifer sein Vorhaben sehr erleichtert. Außerdem ist der Angreifer jetzt im Besitz einer Liste der angreifbaren Rechner.
- 3. *Auswertung:* Für die nächsten Schritte muss der Angreifer eine Verbindung aufbauen und somit in den aktiven Teil des Angriffs übergehen, bei dem er Benutzerkonten mit Passwörtern und andere Zugangsmöglichkeiten testet. Solche Zugriffe sollten protokolliert und erkannt werden, da man ab dem Auftreten solcher Ereignisse mit Angriffen rechnen muß. Da Angreifer meist sehr viel Zeit haben, ist es wichtig diese zu erkennen und ihre Zugriffe zu verhindern, da sie nach erfolgreichem Eindringen in das System mit überall erhältlichen Tools (die in den folgenden Kapiteln zum Teil erläutert werden) ihre Machtstellung ausbauen und großen Schaden anrichten können.
- 4. *Durchführung ihrer Vorhaben:* Beispielsweise Informationsspionage, Löschen von Daten oder Unbrauchbarmachung der Server, Nutzung kompromittierter Rechner zur Durchführung von Distributed-Denial-of-Service-Attacken (DDoS), Installation von Hintertüren, um später leicht in das System eindringen zu können, usw.

Vor diesem Hintergrund erlangt die Deaktivierung der Ports und die Sicherung der Zugänge eine zentrale Rolle, da ein Angreifer, der nicht erkennen kann was für ein System er vor sich hat, auch schlechter die Tools auswählen kann, die erfolgreich wären und ihm den Zugriff ermöglichen würden. Außerdem schränkt man dadurch die Arten und Möglichkeiten des Eindringens in das System erheblich ein und muss zudem weniger potentielle Angriffspunkte überwachen.
Viele der in diesem Kapitel erwähnten Zusammenhänge und Erläuterungen stammen aus [KUR01].

3.1 Passwortangriffe

Jeder Server bietet an irgendeiner Stelle einen Zugang zu Serverdiensten für autorisierte Benutzer. Die Anmeldung erfolgt meist in Form eines Benutzernamens und eines Passwortes, die der Benutzer in ein Textfeld eingibt und sich damit authentifiziert. Hat ein Angreifer Zugang zu dieser Anmeldung, kann er natürlich genauso einen Namen und ein Passwort eingeben und hoffen, die richtige Kombination zu verwenden. Da der Benutzername häufig relativ einfach ist (root, Administrator, Name der Mitarbeiter), muss er sich nur noch um das Passwort kümmern.
Nun wird ein Angreifer nicht Passwörter eintippen und durchprobieren sondern ein geeignetes Programm schreiben oder verwenden, dass die Anmeldeversuche automatisch durchführt.

Der Wörterbuch-Angriff

Benutzer haben die Angewohnheit, Passwörter zu verwenden, die sie sich leicht merken können. Diese leicht zu merkenden Passwörter sind meist Namen von Verwandten oder Wörter, die sich in einem Wörterbuch wieder finden lassen.
Der *Wörterbuch-Angriff* verwendet nun ein Wörterbuch, das vielleicht auch Namen enthält, und versucht sich mit einem Benutzernamen und einem Wort aus dem Wörterbuch als Passwort anzumelden. Klappt der Versuch nicht, wird das nächste Wort im Wörterbuch als Passwort verwendet. Je nachdem wie schnell die Verbindung zum Server ist und wie schnell dieser die Anmeldungen bearbeiten kann, wird es nicht lange dauern um das Passwort herauszufinden.
Dieser Angriff hat den entscheidenden Nachteil, dass nur Passwörter gefunden werden, die auch in einem Wörterbuch enthalten sind. Der *Brute-Force Angriff* umgeht dieses Problem mit ziemlich einfachen Mitteln.

Der Brute-Force-Angriff

Auch bei diesem Angriff wird ein Programm verwendet, das bestehende Benutzernamen und Passwörter durchprobiert. Diese werden allerdings keinem Wörterbuch entnommen, sondern durch Kombinationen von Buchstaben und Zahlen erstellt. Dieses kann systematisch geschehen, indem mit dem Passwort „a“ angefangen und das Alphabet durchlaufen wird („b“, „c“ ... „z“). Als nächstes werden dann Passwörter mit zwei Buchstaben probiert („aa“, „ab“, „ac“ ... „az“, „ba“, „bb“, „bc“ ... „zz“). Die andere Methode verwendet zwar die gleichen Passwörter, geht aber nicht der Reihe nach das Alphabet durch, sondern ändert die Reihenfolge scheinbar zufällig.
Mit dieser Methode lassen sich natürlich auch Passwörter finden, die nicht in einem Wörterbuch zu finden sind, sondern aus willkürlichen Zahlen und Buchstaben bestehen und die Auswahl der verwendeten Zeichen kann bei guten Angriffsprogrammen geändert werden. Der große Nachteil besteht darin, dass sehr viele Kombinationen durchsucht werden müssen und dieser Angriff online nicht praktikabel ist.

Offline Angriffe

Die meisten Server speichern Benutzerpasswörter nicht in Klartext auf ihren Speichermedien, sondern verwenden einen *Hash-Wert* für die Passwörter, der gespeichert wird. Der Hash-Wert wird durch eine bestimmte Methode aus dem Passwort generiert und es ist sehr unwahrscheinlich, dass zwei verwendete Passwörter zum gleichen Hash-Wert führen. Meldet sich ein Benutzer

an, wird aus dem eingegebenen Passwort ebenfalls ein Hash-Wert erzeugt. Sind beide Werte identisch, kann davon ausgegangen werden, dass der Benutzer das Passwort weiß.
Kommt ein Angreifer nun in den Besitz dieser Hash-Werte, hat er zwar noch nicht die Passwörter der Benutzer, er kann allerdings einen Wörterbuch- oder Brute-Force-Angriff offline und auf mehreren Computern durchführen, wodurch die Geschwindigkeit enorm gesteigert wird.

Gegenmaßnahmen

Es gibt mehrere Möglichkeiten, sich gegen Online-Passwortangriffe zu schützen. Ein Online-Passwortangriff kann leicht erkannt werden, da viele erfolglose Benutzeranmeldungen in kurzer Zeit erfolgen. Ein Server sollte so konfiguriert werden, dass ein Benutzerkonto nach einer Anzahl von fehlerhaften Anmeldungen gesperrt oder die Wartezeit zwischen zwei möglichen Anmeldungen erhöht wird. Auf jeden Fall sollten solche Fehlversuche protokolliert und das Protokoll dann regelmäßig überwacht werden.
Gegen Offline-Passwortangriffe kann man sich nur insofern schützen, als dass die Hash-Werte nicht in Besitz des Angreifers kommen dürfen. Hat er diese irgendwie bekommen und wurde dies bemerkt, müssen alle Passwörter geändert werden, weil die alten Hash-Werte nicht mehr sicher sind.

Sichere Passwörter

So trivial diese Gegenmaßnahme auch sein mag, so schwierig ist es, sie auch umzusetzen. Die Verwendung von sicheren Passwörtern ist die sicherste Gegenmaßnahme vor Passwort-Angriffen. Dabei sollten folgende Dinge beachtet werden:

- Passwörter dürfen keine Namen und keine wirklichen Wörter enthalten.
- Sie sollten eine Mindestlänge von 6 oder besser 7 Zeichen haben, je nach Betriebssystem kann diese Zahl aber auch variieren. Generell ist ein längeres Passwort auch ein besseres Passwort.
- Passwörter sollten eine Mischung aus Groß- und Kleinbuchstaben, sowie Zahlen enthalten (die Verwendung von Umlauten und Sonderzeichen ist in gemischten Netzwerken allerdings problematisch)
- Weitere Zeichen, wie #, @, !, & usw. erhöhen die Sicherheit.

Es sollte nicht unterschätzt werden, wie wichtig die Verwendung von sicheren Passwörtern ist. Der beste Weg in ein fremdes Betriebssystem ist die Anmeldung als Administrator. Kapitel 5.1.1 geht daher detaillierter auf dieses Thema ein.

3.2 Netzwerk-Angriffe

Die wenigsten Netzwerkprotokolle basieren auf verschlüsseltem oder geschütztem Datenverkehr. Die meisten Daten, die in einem Netzwerk übertragen werden, können von jedem anderen, der sich im gleichen Netzwerk befindet, gelesen oder verändert werden. Netzwerke funktionieren, da sich alle Beteiligten (Betriebssysteme, Hardware, Programme, etc.) an die verwendeten *Netzwerkprotokolle* halten und diese befolgen.

Ein Angreifer muss dies natürlich nicht und kann seine eigene Interpretation eines Netzwerkprotokolls verwenden, das mit dem sonst verwendeten zwar kompatibel ist, dem Angreifer aber mehr Möglichkeiten eröffnet und es ihm erlaubt, den Netzwerkverkehr abzuhören oder zu manipulieren. Diese Techniken werden nicht nur von Angreifern verwendet. Auch Netzwerkadministratoren bedienen sich solcher Mittel um Fehler aufzuspüren oder den Netzwerkverkehr zu überwachen, weshalb viele Betriebssysteme dafür entwickelte Programme gleich mitliefern und es viele kommerzielle Programme zur Netzwerküberwachung gibt.
Natürlich muss der Angreifer Zugriff auf den Netzwerkverkehr haben. Ein Angreifer in New York wird nicht in der Lage sein, den Datenstrom zwischen zwei Systemen in Berlin abzufangen oder mitzuhören. Die Verwendung von öffentlichen Netzwerken erhöht allerdings das Risiko und in einem lokalen Firmennetzwerk ist dieses Problem genauso vorhanden und führt immer noch zu so beliebten Spielen, wie dem Herausfinden des Passworts vom Chef.

Sniffing

Unter *Sniffing* versteht man das Abhören von Netzwerken und das "Mitlesen" oder Aufzeichnen der übertragenen Daten, die eigentlich für jemand anderen gedacht waren. Das Wort „Sniffing“ kommt von den ersten Programmen, die dafür entwickelt wurden und „Sniffer“ genannt wurden. Dabei funktionieren alle Sniffer-Programme nach dem gleichen Prinzip: Normalerweise wertet die Netzwerksoftware des Betriebssystems nur die Netzwerkdaten aus, die als Zieladresse die eigene Netzwerkadresse haben. Dieses Funktion kann wird geändert, woraufhin alle Pakete oder solche mit bestimmten Zieladressen zusätzlich ausgewertet werden.

Auswirkungen

Gute Sniffer-Programme werten die Daten aus, erkennen verwendete Protokolle und bereiten die Daten in leserlicher Form auf. Protokolle, die auf reinen Text basieren, wie z.B. FTP, Telnet und HTTP werden häufig direkt erkannt und interessante Informationen sofort ausgegeben. Da diese Protokolle alle in Klartext übertragen und verwendete Passwörter und Benutzernamen unverschlüsselt übermittelt werden, kann das Sniffer-Programm diese gleich mit ausgeben.
Gerade das FTP-Protokoll wird häufig für die Pflege von Websites bei Providern eingesetzt und die wenigsten Provider unterstützen irgendwelche Verschlüsselungen, so dass solche Zugriffsrechte sehr leicht zu „sniffen“ sind. Aber selbst verschlüsselte Daten können natürlich aufgezeichnet werden und mit einigem oder erheblichem Mehraufwand manchmal auch wieder entschlüsselt werden.

Verändern von Daten (Man-in-the-Middle Angriff)

Etwas schwieriger als das Abhören von Daten ist das Verändern von Daten, die zwischen zwei Systemen ausgetauscht werden. Da diese Funktion natürlich vom Netzwerkprotokoll nur bedingt vorgesehen ist (Router verwenden diese Methode, nur werden die Daten nicht verändert), muss sich der Angreifer einiger Tricks bedienen und auch hier ist der Zugriff auf das lokale Netzwerk nötig.
Der Angreifer muss zuerst verhindern, dass die Daten das eigentliche Ziel erreichen. Dazu muss er das sendende System dazu bringen, die Daten zu ihm zu schicken, oder den Netzwerkverkehr zwischen den beiden Systemen unterbrechen. Netzwerkrouter können ebenfalls dafür eingesetzt werden, da diese den Datenstrom ohnehin bearbeiten müssen.

Kann der Sender keine Daten mehr direkt an den Empfänger senden, muss der Angreifer diese Rolle übernehmen und sich als Sender ausgeben (Spoofing). Die Daten, die der Angreifer nun weiterleitet, können verändert werden, wodurch er sein Ziel erreicht hat.

Auswirkungen

Die Veränderung von Daten kann viele Auswirkungen haben. Zum Beispiel kann ein Banküberweisungsauftrag verändert werden, wodurch eine falsche Summe überwiesen oder der Empfänger geändert wird.
E-Mails können verändert werden und Texte enthalten, die der Empfänger nicht bekommen sollte und die er vielleicht falsch verstehen würde. Webseiten, die gerade per FTP auf den Server überspielt werden, können während der Übertragung geändert werden. Feststellbar ist, dass die Auswirkungen dieses Angriffs sehr vielfältig sein können und nur von der Phantasie eines Angreifers eingeschränkt werden.

Gegenmaßnahmen

Es gibt eigentlich nur eine wirksame Gegenmaßnahme gegen diese Angriffe. Die Verschlüsselung des Datenstroms verhindert ein einfaches Mitlesen der Daten und durch das Signieren der Daten durch den Sender, kann der Empfänger sicher sein, dass die Daten nicht verändert wurden. Dies kann auf verschiedene Weise geschehen und entweder ins Netzwerkprotokoll integriert werden (z.B. IPSec) oder durch die Anwendungen vorgenommen werden (z.B. SSL/TLS).
Wichtig ist, eine ausreichend starke Verschlüsselung zu verwenden, damit der Angreifer die Daten nicht entschlüsseln kann.
Interne Netzwerke können durch die Verwendung von Netzwerkswitches zwar nicht zu 100% geschützt werden, da auch diese Technik nicht sicher vor solchen Angriffen schützt, aber es wird für den Angreifer schwieriger den Datenstrom abzuhören. Neue Netzwerktechnologien, wie Wireless LAN, also Funknetze, machen es dem Angreifer aber auch wieder leichter, Angriffe durchzuführen, da er nicht einmal einen direkten Kontakt zum Netzwerk haben muss, sondern sich einfach auf den Firmenparkplatz stellen kann. Auch wenn diese Funknetze eine eingebaute Verschlüsselung besitzen, hat sich gezeigt, dass diese nicht ausreichend hoch ist und die Verwendung von sicheren Netzwerkprotokollen dringend empfohlen wird.

3.3 Port-Scanning

Durch das Footprinting hat der Angreifer bereits die erreichbaren Systeme gefunden und geht jetzt in die Testphase über, um die erreichbaren und somit aktiven Rechner zu finden. Dies macht man mit Hilfe von vielen Tools, unter anderem Ping-Suchläufen, Port-Scans und automatischen Suchtools, die viele dieser Funktionen vereinen. Mit diesen Maßnahmen findet er die von seinem Standpunkt aus angreifbaren Rechner heraus. Die verschiedenen Methoden, die zur Erreichung dieses Ziels erforderlich sind, sollen hier kurz skizziert werden.

Ping-Suchläufe

Mit *Ping-Suchläufen* wird ein großer Adressbereich ange„pingt", dabei wird normalerweise ein SYN-Paket zum Zielrechner gesendet, dieser antwortet mit einem SYN-ACK-Paket und dieses wird dann mit einem ACK-Paket beantwortet. Damit sieht der Angreifer welche Adressen antworten und er besitzt am Ende eine Liste mit angreifbaren Rechnern. Tools wie ‚fping' für UNIX erlauben

es, viele IP-Adressen parallel anzupingen, statt, wie das einfache ‚ping' Programm, auf eine Antwort zu warten, bevor es den nächsten Ping losschickt. Für Windows gibt es ‚Pinger' von Rhino9, das ebenfalls parallele pings ermöglicht. „ICMP[27] stellt Troubleshooting-Funktionen und Fehlerberichte für Pakete zur Verfügung, die nicht übertragen werden konnten,...dies macht IP zu einem unzuverlässigen Protokoll" [SCH01]. ICMP ist das Protokoll, das für Antworten auf Ping-Anfragen zuständig ist, insofern ist es teilweise wünschenswert, diese Antworten zurückzuhalten. Es gibt Firewalls und Router die ICMP blockieren. Diese sind allerdings beim Einsatz von TCP-pings oder Port-Scans meist wirkungslos, da sie nicht mit ICMP arbeiten und sehr oft durchgelassen werden. Außerdem bieten Tools wie ‚hping' die Möglichkeit, Pakete zu fragmentieren, dadurch können sie von den Routern nicht mehr erkannt werden und kommen zurück. An dieser Stelle muss gesagt werden, dass langsame oder Frame-Relay (Satelliten) Verbindungen leicht überlastet werden können, etwa durch das Anpingen einer Broadcast-Adresse, z.B. 192.168.1.255, was zu einer Denial-of-Service-Fehlermeldung führen kann. Ping-Suchläufe sind nur für kleine bis mittlere Netzwerke geeignet, da sie bei großen Netzwerken sehr lange dauern können.

Port-Scans

Mit *Port-Scans* fragt man für jede gültige IP-Adresse eines Zielnetzwerks die gängigen Ports ab und kann durch die offenen Ports meist erkennen mit was für einem System man es zu tun hat. Der Angreifer wird die TCP- und UDP-Ports scannen, um zu sehen, um welches Betriebssystem es sich handelt und welche offenen Ports es gibt, die den Status „abhören" besitzen, da er über diese eventuell Zugriff auf das System bekommen könnte. Man kann über die Versionen der eingesetzten Software natürlich auch einfach auf Sicherheitslücken, die überall abrufbar und dokumentiert sind, schließen, für die die erfolgreichen Angriffe bereits bekannt sind.

Es existieren verschiedene Port-Scan-Typen, die hier erläutert werden sollen.

- Ein *TCP-Connect-Scan* baut eine Verbindung inklusive vollständigem Handshake (SYN, SYN/ACK, ACK) auf. Dieses ist für den Zielrechner leicht zu erkennen und sollte Warnmeldungen generieren oder zumindest für Aufmerksamkeit sorgen.
- Ein *TCP-SYN-Scan* führt kein vollständiges Handshake durch. Es wird ein SYN-Paket übertragen und wenn ein SYN/ACK Paket zurückkommt, wird ein RST/ACK-Paket übertragen, welches eigentlich von einem deaktivierten Port als Antwort auf ein SYN gesendet wird und dies lässt keine Verbindung zustande kommen. Wenn ein RST/ACK-Paket vom Ziel zurückkommt, ist der Port deaktiviert. Dieses Vorgehen ist viel unauffälliger als ein vollständiger Handshake und damit schwerer zu erkennen, obwohl es für den Angreifer zum gleichen Erfolg führt.
- Ein *TCP-FIN-Scan* überträgt ein FIN-Paket, das normalerweise für die Beendigung einer Verbindung benutzt wird. Diese Art funktioniert nur bei UNIX und liefert dann ein RST für alle geschlossenen Ports (nach [RFC793]).
- Ein *TCP-Xmas-Scan* überträgt ein FIN-, ein URG- und ein PUSH-Paket und der Zielrechner liefert daraufhin RST-Pakete für alle geschlossenen Ports (nach [RFC793]).
- Ein *TCP-Null-Scan* schaltet alle Flaggen aus, nach [RFC793] müsste ein RST-Paket für alle geschlossenen Ports zurückkommen.

27 Internet Control Message Protocol

- Ein *TCP-ACK-Scan* wird zum Erkennen der Sicherheitsregeln von Firewalls eingesetzt. Ein einfacher Paketfilter, der nur bestätigte Verbindungen (ACK-Bit) durchlässt, wird auf diese Weise erkannt oder falls der Versuch nicht erfolgreich ist, kann der Angreifer auf eine intelligente Firewall schließen.
- Ein *TCP-Windows-Scan* nutzt eine Anomalie an TCP-Fenstergrößen aus und kann hiermit offene und gefilterte/ungefilterte Ports erkennen.
- Ein *UDP-Scan* überträgt ein UDP-Paket. Bei keiner Antwort ist der Port aktiv, bei einer „ICMP Port Unreachable" Antwort ist der Port inaktiv. UDP ist verbindungslos, deswegen können solche Scans sehr lange dauern, hängen stark von der Netzwerklast ab und einige Antworten könnten auch nicht ankommen.

Mit Tools wie ‚icmpenum' für UNIX ist es möglich, *gespoofte* Pakete mit gefälschter Absenderadresse zum Erkunden von Netzwerken zu versenden, um die eigene Identität zu verschleiern.

Scan-Tools für Windows 2000 sind unter anderem ‚Superscan' (Freeware) oder ‚NetScanTools Pro 2000'.

Gegenmaßnahmen

Es sind Tools erhältlich, die Aktivitäten wie Port-Scans erkennen und dann durch Warnmeldungen, E-mails oder Pagernachrichten Alarmmeldungen generieren. Diese Funktionalität ist zum Schutz der eigenen Systeme und zur weiteren Planung sehr wichtig, da man meist ab diesem Zeitpunkt mit einem Angriff rechnen muss.

Solche Tools für Windows 2000 sind ‚Genius', ‚BlackICE', das erste agentenbasierte IDS (Intrusion Detection System) oder ‚ZoneAlarm', das IDS- und Firewall-Funktionalität in einem bietet.

3.4 Spoofing

Unter *Spoofing* versteht man das Fälschen der eigenen IP-Pakete mit Absenderadressen von anderen, um eine fremde Identität vorzutäuschen und auf diese Weise durch Firewalls hindurchzugelangen und an Informationen zu kommen, die nicht für einen bestimmt sind, oder Informationen unter Vorgabe einer falschen Identität zu senden. Eine Firewall überprüft ankommende Pakete auf ihre Absenderadresse und entscheidet durch diese Information, wie mit den ankommenden Paketen zu verfahren ist. Es handelt sich somit um eine unsichere Art der Authentifizierung.

Pakete in TCP/IP-Netzwerken enthalten die IP-Adressen des Quell- und Zielsystems, dies sind die Quell-Portnummer und die Ziel-Portnummer. Des Weiteren enthalten sie eine Sequenznummer, eine Bestätigungsnummer und einige Flags.

Um sinnvolles Spoofing zu betreiben, muss man die richtige Quell-Portnummer und vor allem die richtige Sequenznummer erraten, da der Zielrechner ansonsten die Verbindung ablehnt. Beim Verbindungsaufbau sendet der Client ein Paket, daraufhin sendet der Server ein Paket mit der Sequenznummer plus eins zurück und der Client sendet erneut ein Paket der Servernummer plus eins.

Das Schwierige ist für einen Angreifer das Beantworten des Serverpaketes plus eins. Deshalb hören die meisten Angreifer den Netzwerkverkehr durch Sniffing ab, damit sie die Sequenznummern kennen.

Wenn man dem eigenen Rechner die Quell-Portnummer des einen Kommunikationspartners gibt, ist man in der Lage, an die Pakete, die für ihn bestimmt sind, zu gelangen. Man kann auf diese Weise ebenfalls Pakete senden, indem man die Sequenznummern in den abgefangenen Paketen fortführt. Zusätzlich werden Angreifer eventuell eine Denial-of-Service-Attacke auf den Sender tätigen, um ihn so am Senden von Paketen zu hindern und ihre eigenen Pakete an den Empfänger schicken. Dies ist bekannt als Man-In-The-Middle–Attacke. Wurde bei der übernommenen Kommunikation zuvor eine Anmeldung durchgeführt, ist es sogar möglich auf Dateien zuzugreifen, die von den ursprünglichen Benutzern freigegeben wurden.

Weitere Spoofing-Typen

Beim *ARP-Spoofing* sendet der Angreifer falsche Mapping Informationen an das Ziel und seinen Cache, um zu erreichen, dass eine vertraute IP-Adresse mit seiner eigenen MAC[28]-Adresse verbunden wird. Dadurch werden die Pakete an seine MAC-Adresse und somit an ihn gesendet.

Durch *DNS-Spoofing* verschafft sich der Angreifer Zugang zum DNS-Server und ändert gezielt Zuordnungen zwischen Hostnamen und IP-Adressen. Somit kann er Netzwerkverkehr umleiten und Daten abhören oder Zugänge zu anderen Rechnern öffnen.

Gegenmaßnahmen

Eine der wichtigsten Gegenmaßnahmen gegen normales Spoofing ist der Verzicht auf Authentifizierung über IP-Adressen und stattdessen der Einsatz anderer kryptografischer Verfahren, die Authentifizierung und Sitzungen verschlüsseln. Möglich wird dies beispielsweise durch den Einsatz von IPSec.

Gegen DNS-Spoofing kann regelmäßig oder bei Verdacht ein Vergleich der Daten von mehreren DNS-Servern durchgeführt und auf verschiedene Resultate geachtet und reagiert werden, indem die richtigen Zuordnungen wiederhergestellt werden.

Eine wirksame Maßnahme gegen ARP-Spoofing ist die Festlegung der MAC-Adressen in den Routern und das Sperren von Änderungen in ihnen, so dass eindeutig festgelegt ist, wohin die Pakete von den Routern geleitet werden sollen.

Fazit

Das Spoofing wird erst durch die Tatsache ermöglicht, dass die Quell-Portnummer vom Sender selbst eingetragen wird, insofern kann ein Angreifer jede Quell-Portnummer in seine IP-Pakete eintragen. Dies ist im Aufbau des IP-Protokolls begründet.

---

28 weltweit eindeutige Adresse, die in der Netzwerkkartenhardware gespeichert ist

3.5 Connection Hijacking

Unter *Connection Hijacking* versteht man das Übernehmen einer bestehenden Sitzung unter Ausschließung des ursprünglichen Verbindungspartners.

Es ist möglich, durch das Abhören von Server und Client, die Pakete so zu verändern, dass man nach der Anmeldung und Authentifizierung des Clients die Verbindung übernimmt und eingeloggt ist, um dann Aktionen auf dem Server als der vermeintliche Benutzer durchzuführen.

Solche Angriffe sind nur durch die Schwächen von TCP möglich, können aber effizient durchgeführt werden. Man kann sie jedoch stark reduzieren und eventuell unterbinden, wenn man verschlüsselte Kommunikationsprotokolle wie IPSec oder SSH[29] benutzt.

Eine Variante ist das *Session Hijacking*. Früher dachte man, dass man mit Switches, die die Netzpakete nur vom Server zum Client und nicht durch das gesamte Netzwerk leiten, großen Schutz vor diesen Problemen hätte, findige Hacker haben aber auch hierfür Mittel und Wege gefunden und Tools entwickelt. Das Tool ‚dsniff' unter UNIX kann den gesamten Netzwerkverkehr zu dem ausführenden Rechner leiten.

Windows-Tools hierfür sind z.B. ‚Juggernaut' von Mike Schiffmann (http://www.packetfactory.net) oder ‚Hunt' von Pavel Krauz (http://www.cri.cz/kra/index.html).

3.6 Denial-of-Service-Angriffe, Distributed-DoS

Ein *Denial-of-Service-Angriff* (DoS) zielt auf die Verweigerung einer Dienstleistung der Hard- oder Software des Zielrechners ab und versucht ihn unerreichbar für Anwender zu machen, indem dieser Dienste für berechtigte oder unberechtigte Benutzer verweigert.

Verschiedene DoS-Angriffstypen

Es gibt verschiedene Arten von DoS-Angriffen, wobei immer neue Varianten auftauchen. Hier soll nur eine Auswahl allgemeiner Art erscheinen, in der die gängigsten Angriffsvarianten aufgeführt sind.

Eine der beliebtesten Arten ist das *Aufzehren der Bandbreite*. Dafür gibt es zwei Möglichkeiten: 1. Der Angreifer hat mehr Bandbreite als das Ziel und kann es überfluten. Hierzu kann sich der Angreifer auch in ein bandbreitenstarkes Netz einhacken und den Angriff von dort aus starten. 2. Verstärken des Angriffs durch Verwendung mehrerer Quellen mit einem *Distributed-Denial-of-Service-Angriff* (DDoS), der zu den verteilten Angriffen zählt und bei dem die Quellrechner des Angriffs meist mit Hilfe von Trojanern dazu gebracht werden, gleichzeitig Daten an das Netzwerk des Ziels zu senden und so viel mehr Netzwerkverkehr generieren, als es dem Angreifer mit seiner eigenen Netzwerkstruktur möglich wäre.

29 Secure Shell

Sehr großer Beliebtheit erfreut sich auch das *Aufbrauchen von Ressourcen*. Dabei ist eine Variante das Aufbrauchen von System- und nicht Netzwerkressourcen. Der Angreifer hat ein gewisses Kontingent an Ressourcen, belegt aber zusätzliche Ressourcen und füllt das Dateisystem oder lässt Prozesse hängen und führt damit den Absturz des Systems herbei. Häufig geschehen solche Angriffe durch das Herbeiführen von *Pufferüberläufen*. Ein Angreifer kann außerdem die Netzwerkressourcen eines Rechners aufbrauchen, indem er den Rechner mit ungültigem Datenverkehr belastet und so die normale Funktionalität behindert. Dies kann sogar zum Absturz des Zielrechners führen. Er kann beispielsweise sehr viele TCP-Verbindungen anfordern, damit die Warteschlangen füllen und somit den Zugriff für andere Benutzer unmöglich machen. Des Weiteren ist es möglich, Computer oder Netzwerke mit Datenverkehr zu überschwemmen, bis es zum Überlauf kommt. Eine weitere Variante ist, die Netzwerkstruktur und nicht das System anzugreifen, indem man den oder die Router zum Absturz bringt und somit die Netzwerkinfrastruktur lahmlegt. Es sind einige Fehler in den Betriebssystemen auf Routern, beispielsweise von Cisco, bekannt geworden und es ist nicht unbedingt kompliziert, die Art der verwendeten Routerhardware herauszufinden.

Programmierfehler bilden eine weitere Kategorie der Probleme, die DoS-Angriffe erst möglich machen. Das Hervorrufen von Ausnahmebedingungen, die nicht abgefangen werden, kann durch einen Angreifer geschehen, indem er nicht vorgesehene Daten an Komponenten sendet, z.B. keine nach den RFCs gültigen Netzwerkpakete, um zu sehen, ob der Netzwerkstapel die Fehlermeldung verarbeiten kann oder ob das System mit einer Ausnahmebedingung abstürzt. Beispielsweise zu große Pakete mit zu großen Puffern können zu einem Pufferüberlauf führen, der das System abstürzen lässt oder das Ausführen von Befehlen ermöglichen kann. Dies ist auch in den Chips selber möglich. Ein bekannter Pentium-f00f-DoS-Angriff bringt den Prozessor zum Absturz, wenn man auf ihm den ungültigen Befehl ‚0xf00fc7c8' ausführt.

Bei *Routing- und DNS-Angriffen* wird die Routing-Tabelle eines Netzwerks manipuliert, um das Netzwerk zu isolieren. Das RIP v1 (Routing Information Protocol) und das BGP v4 (Border Gateway Protocol) besitzen nur eine sehr schwache Authentifizierung und sind daher durch Spoofing der eigenen IP-Adresse und eine anschließende Änderung der Routen leicht angreifbar. Die Daten des Opfers landen dabei irgendwo, nur nicht dort wo sie hin sollen. Beim DNS-Angriff trägt der Angreifer im DNS-Server falsche IP-Adressinformationen ein, die bei der Ausführung einer Suchanfrage dazu führen, dass ein DNS-Server dadurch ins Nirgendwo geleitet wird.

Es existieren *generische DoS-Angriffe*, sie sind plattformübergreifend und bestehen meist aus Bandbreiten- oder Ressourcen-Angriffen. Ihr hauptsächlicher Angriffspunkt sind Manipulationen des Protokolls, wie z.B. E-Mail-Bombing, bei dem man eine sehr große Anzahl an E-Mails kontinuierlich an eine E-Mail-Adresse sendet und damit den Mailserver des Ziels überlastet und ihn eventuell zum Absturz bringt.

Distributed-DoS-Angriffe setzen voraus, dass man auf möglichst vielen Systemen Administrator-Rechte erobert, um DDoS-Software auf allen kompromittierten Rechnern zu installieren, die dann auf „Befehle" wartet, um dann einen Angriff mit allen Systemen auf einmal zu starten. Beispiele für solche Software sind ‚TFN' (Tribe Flood Network), ‚TFN2k' (TFN für Windows 2000), ‚Trinoo', ‚Stacheldraht' und ‚WinTrinoo'.

Es gibt *Remote-* und *Lokale-DoS-Angriffe*. Beide sind gleichermaßen gefährlich, wobei die lokalen natürlich einen physischen Zugriff zu dem Zielrechner voraussetzen. Für Windows NT 4.0, den Terminal Server und ‚proquota.exe' kann es beispielsweise zur Kernel-Panic, einer Kernel Ausnahmebedingung, kommen, die zum Absturz des Systems führt.

Denkbar ist auch ein Szenario, bei dem ein Angreifer einen DoS-Angriff einleiten könnte, um aus diesem weiteren Nutzen zu ziehen, als nur die bloße Verweigerung eines Dienstes des Zielrechners. Vorausgesetzt er hat Veränderungen am System vorgenommen, beispielsweise Software installiert, und benötigt für diese zum Wirksamwerden einen Neustart, dann könnte er mit einem DoS-Angriff erreichen, dass der Administrator das System neu bootet und auf diese Weise seine Tools startet. Administratoren rechnen meist nicht damit, dass ein anderer Zweck als Denial-of-Service hinter einem solchen Angriff steckt oder bemerken nicht einmal, dass es ein Angriff war, sondern denken, der Rechner sei abgestürzt und starten ihn einfach neu.

Spezielle Windows 2000 Angriffe

Selbstverständlich sind auch Angriffe bekannt, die speziell auf die Windows 2000 Architektur zugeschnitten sind. An dieser Stelle wird keine vollständige Liste angeboten, sondern eher ein Einblick in die momentane Sicherheitssituation gewährt.

Werden etwa *speziell missgeformte Pakete* (malformed Packets) an einen Windows 2000 Rechner gesendet, kann das dazu führen, dass der Rechner durch die Reassemblierung der Pakete ausgelastet wird und im Extremfall abstürzt (siehe auch 4.1.5 Netzwerk).

Eine trickreiche Methode, um die Anmeldesicherheit zu untergraben, besteht in einer SYN-Flooding-Attacke, bei der permanent SYN-Pakete auf Port 88 gesendet werden, der den Kerberos-Port darstellt, um den Server an einer Kerberos-Anmeldungsmöglichkeit zu hindern. Windows 2000 wurde so implementiert, dass bei einem Ausfall von Kerberos auf den alten NTLM zurückgegriffen wird, was dem Angreifer bekanntlich einen viel einfacheren Zugriff ermöglicht [URL18].

Ein *Telnet-Server* DoS-Angriff kann durch Senden von binären Nullen an diesen durchgeführt werden. Er bringt den Dienst und den Server zum Absturz und veranlasst damit ständig Neustarts, da dies von Microsoft so festgelegt wurde. Bei der Standardinstallation von Windows 2000 ist der Telnet-Server allerdings deaktiviert, hier besteht also keine Gefahr.

Denial-of-Service-Angriffe über *NetBIOS-Namensserver-Protokoll-Spoofing* sind nur vom lokalen Netzwerk aus möglich, da der NBNS (NetBIOS Name Service) nicht routingfähig ist und somit nicht aus dem lokalen Netzwerk herausgelangt. Mit einem „NetBIOS-Name-Release-Request" an den Port NBNS, der bei UDP 137 ist, wird der Server gezwungen, seinen eigenen Namen in Frage zu stellen und bedient das NetBIOS-Netzwerk danach nicht mehr. Damit können die Benutzer nicht mehr auf diesen Server zugreifen oder seine Funktionen nutzen.

Man kann mit DoS-Angriffen auch die Administratoren der Systeme *von anderen Angriffen ablenken*, die man gleichzeitig durchführt. Während sich die Administratoren um die Schadensbegrenzung des DoS-Angriff kümmern, kann der Angreifer seine Vorhaben an anderer Stelle vorantreiben, ohne dass er eventuell behelligt wird, was ohne DoS-Angriff im Hintergrund wahrscheinlich bemerkt würde. Außerdem werden die Administratoren vielleicht auch nicht später nach anderen Angriffshinweisen suchen und somit bleiben die anderen Angriffe unentdeckt.

Gegenmaßnahmen

Es gibt in Windows 2000 Möglichkeiten, um Denial-of-Service-Attacken bis zu einem gewissen Grade abzuwehren. Sie können zum Teil durch Änderungen in Registrierungsschlüsselwerten, die auch von Microsoft-Patches vorgenommen werden, entkräften werden, indem der TCP/IP-Stapel gegen diese Angriffe geschützt wird.

In folgenden Schlüsseln kann man hierfür Einstellungen vornehmen:

Im *SYN AttackProtectionFailure* Registrierungsschlüssel kann man einige Einstellungen vornehmen, die das Standardverhalten für die Antwort auf SYN-Pakete verändern. Wenn SYN AttackProtectionFailure auf den Wert 0 gesetzt ist, ist der Schutzmechanismus deaktiviert, bei 1 wird die Verbindung erst bei Erhalt des ACK-Paketes erstellt und bei 2 wird der Winsock Kernelmodustreiber erst benachrichtigt, wenn das drei-Wege-Handshake stattgefunden hat, somit werden DoS-Angriffe durch unvollständigen Verbindungsaufbau entkräftet.

Es gibt drei Registrierungsschlüssel, die das Verhalten bestimmen: *TcpMaxHalfOpen* legt die maximale Anzahl der SYN-Anfragen, die noch nicht durch ein ACK bestätigt wurden, fest. *TcpMaxHalfOpenedRetried* definiert die Anzahl der gesendeten SYN/ACK-Pakete, bevor das System in den SYN-Attack Status wechselt. *TcpMaxPortsExhausted* legt die Anzahl der abgelehnten Anfragen, ab der in den SYN-Attack Status gewechselt wird, fest.

Außerdem gibt es noch *TcpMaxConnectResponseRetransmissions*, die die Anzahl der Wiederholungen der SYN/ACK-Pakete spezifizieren. Diese werden standardmäßig im Abstand 3, 6 und 12 Sekunden gesendet und sind drei Stück, danach wird die Anfrage verworfen, welches normalerweise 45 Sekunden dauert. Wenn man Opfer von SYN-Attacken ist, sollte man diesen Wert auf 1 setzen, dann wird die Anfrage nach 9 Sekunden verworfen. Man kann den Wert auch auf 0 setzen, das ist zwar nicht freundlich für Benutzer, die schlechte Netzwerke und Ping-Zeiten haben, aber sicher gegen Angriffe.

Gegen den *Telnet-Server DoS-Angriff* gibt es einen Patch bei Microsoft, der nicht im Service Pack 1 enthalten ist.

Um den DoS-Angriff über *NetBIOS-Namensserver-Protokoll-Spoofing* zu verhindern, gibt es einen Patch bei Microsoft, der nicht zum Service Pack 1 gehört und der verhindert, dass die Requests angenommen werden. Zusätzlich sollte man in der Firewall Port 137 schließen oder aber am besten NetBIOS komplett deaktivieren, vor allem wenn man es nicht braucht.

Auch für Router gibt es Patches oder zumindest Anleitungen zur sicheren Konfiguration. Auf der sicheren Seite ist man hier mit Routern, die keine Management-Funktionalität anbieten, da sie keine Eingriffsmöglichkeiten bieten, mit denen ein Angreifer sie umkonfigurieren könnte.

Als zusätzliche Sicherheitsmaßnahmen kann man den IPSec-IP-Paketfilter verwenden, der Pakete von unbekannten Adressen verwirft und somit eine Art rudimentäre Firewall darstellt, von der allerdings noch nicht bekannt ist, wie effizient sie ist.

Fazit

Denial-of-Service-Angriffe und vor allem ihre DDoS-Variante stellen momentan ein großes Sicherheitsproblem dar. Sie sind mit überall erhältlichen Tools relativ leicht durchzuführen und richten sehr großen Schaden an. Vor allem bei jungen Hackern erfreuen sie sich großer Beliebtheit, da das Resultat eines DoS-Angriffs sofort sichtbar ist und sie somit für sich Erfolgserlebnisse verbuchen können.
Das Ziel eines solchen Angriffs besteht immer in einer Abtrennung vom Netzwerk oder der Verhinderung einer Dienstleistung.
Glücklicherweise funktionieren viele der verbreiteten DoS-Tools wie ‚teardrop' oder ‚land' bei Windows 2000 nicht mehr. Eine aktive Überflutung von Ports, wie sie nach wie vor sehr beliebt ist, da sie einfach zu realisieren ist, macht dem System nichts mehr aus. Mit den Optionen der Konfiguration in den Registrierungsschlüsseln bietet Microsoft in Windows 2000 einige Möglichkeiten, um diese Gefahren zumindest ein wenig einzuschränken.

3.7 Replay-Attacken

Eine *Replay-Attacke* besteht aus dem Aufzeichnen eines Datenpaketstroms, der eine komplette Kommunikation darstellt und dem anschließenden nochmaligen Senden dieses Paketstroms. Gelingt es einem Angreifer eine komplette Sitzung eines Clients mit einem Server auf Protokollebene aufzuzeichnen, ist er in der Lage zu einem späteren Zeitpunkt, wenn der Client wieder abgemeldet ist, diesen Paketstrom noch einmal zu senden. Hiermit kann man beispielsweise eine Banküberweisungstransaktion mehrmals durchführen.

Gegenmaßnahmen

Eine sinnvolle Gegenmaßnahme, um dieses Problem in den Griff zu bekommen bietet IPSec durch die nutzbare Anti-replay Funktionalität, mit der eindeutige Pakete erstellt und vom Kommunikationspartner erwartet werden.

3.8 Trojaner

Der Name „Trojaner" stammt von dem legendären trojanischen Pferd, das innen hohl war und den Angreifern den Zugang zu Troja ermöglichte. Trojaner sind bösartige Programme, die einen Benutzer glauben lassen, etwas anderes zu sein, aber Programmcode des Angreifers enthalten.
Dabei kann ein Trojaner ein kleines Spiel, ein nützliches Programm oder ein Programm sein, das angeblich Trojaner auffinden soll. Ein Angreifer kann solche Programme für viele Dinge verwenden und unterschiedliche Software in dem Trojaner verstecken. Für ihn ist es natürlich einfacher, wenn seine Angriffssoftware auf dem betreffenden Computer durch einen Anwender selbst installiert und ausgeführt wird.

Auswirkungen

Startet ein Benutzer solch ein Programm, ist es meist zu spät. Ein gestarteter Trojaner wird mit den Sicherheitsrechten des Benutzer ausgeführt und kann Daten manipulieren oder löschen, sich selbst oder andere Programme im System installieren und Benutzerkonten einrichten, die ein Angreifer dann verwenden kann. Dies können auch weitere Administratorkonten sein, wenn der Benutzer, der den Trojaner startet, über genügend Rechte verfügt oder der Trojaner sich diese Rechte irgendwie selbst beschaffen kann.
Dabei muss der Trojaner nicht unbedingt neue Konten anlegen. Hat das Trojaner-Programm Zugriff auf die Hash-Werte der Benutzerpasswörter, kann es versuchen, diese direkt an den Angreifer zu schicken, der diese dann lokal entschlüsseln kann und dadurch in den Besitz der Passwörter kommt. Die Installation eines Backdoors-Programm, das Tastaturanschläge aufzeichnet, kann natürlich den gleichen Effekt haben und eingetippte Passwörter direkt aufzeichnen und dem Angreifer zur Verfügung stellen.

Herkunft von Trojanern

Trojaner können von Benutzern eingeschleust oder als ein E-Mail-Anhang verschickt werden, der dann von einem nichts ahnenden Benutzer ausgeführt wird. Gute Trojaner versuchen dabei möglichst attraktiv zu sein, so dass sie sich schnell im Netzwerk ausbreiten. Webseiten können ebenfalls Trojaner im System einschleusen, wenn Sicherheitseinstellungen in einem Webbrowser falsch konfiguriert sind. Ein Angreifer kann es auch geschafft haben, andere Programme zu ersetzen (z.B. das Programm ‚notepad.exe' unter Windows), die bei Verwendung des Ursprungsprogramm ausgeführt werden und den Trojaner installieren.

Gegenmaßnahmen

Das Ausführen von unbekannten E-Mail-Anhängen ist unbedingt zu vermeiden. Leider erledigen E-Mail-Programme dies manchmal auch ohne den Benutzer darüber zu informieren, so dass solche Programme und Browser dementsprechend konfiguriert werden müssen und sich die Ausführung von Programmen oder Scripten vom Benutzer bestätigen lassen. Aber auch das Ausführen von Programmen, die aus bekannter Quelle stammen, kann problematisch sein, wenn die Quelle schon infiziert wurde (und das vielleicht gar nicht weiß).
Antiviren-Programme können aktuelle und bekannte Trojaner identifizieren, eigens für einen Angriff entwickelte Trojaner dagegen meist nicht. Generell sollte man allen Dateien oder Programmen eher skeptisch gegenüber eingestellt sein und kein Risiko eingehen.

3.9 Rootkits

Rootkits werden als die ultimative Angriffsart gesehen. Ein Rootkit ist im Betriebssystem installierter Code, der auch aus manipulierten Betriebssystemdateien bestehen kann, von dem man meint, dass er der originale Code ist. Ebenso wie Trojaner sind es Anwendungen oder Dienste, die man nur sehr schwer entdecken kann.

Schon ein kurzes Aufflackern der Eingabeaufforderung sollte einen Systemadministrator stutzig machen. Insgesamt gesehen sollte jede Form einer Veränderung des gewohnten oder erwarteten Verhaltensmusters eine Analyse nach sich ziehen.

Es existiert ein Rootkit von Greg Hoglund unter http://www.rootkit.com welches über „Funktions-Hooking" den NT-Kernel manipuliert und in Aufrufe eingreift, um beispielsweise Trojaner anstatt der ursprünglich aufgerufenen Anwendungen ausführen. Somit ist man sich nie sicher, ob der ausgeführte Code der originale und gewünschte ist.

Bei der Erkennung eines solchen Zustandes bleibt einem nur eine Wahl. Vorausgesetzt man verfügt über eine gute Backup-Strategie und eine Desaster Recovery Ablaufliste, kann man den Schaden meist schnell und effektiv beheben. Da man sich leider nicht sicher sein kann, wann der Trojaner oder das Rootkit in das System gelangt ist, muss man das System von den Original-Datenträgern neu installieren, die Sicherheit durch alle nötigen Patches gewährleisten und die Einstellungen im System entsprechend der vorherigen oder auch einer erweiterten Konfiguration vornehmen. Zum Schluss lädt man vom Backup seine Daten zurück. Man kann natürlich auch nach der Installations- und Konfigurationsprozedur ein Image des Systems, das ein rücksicherbares Backup einschließlich Bootinformationen darstellt, erstellen und dieses schreibgeschützt aufbewahren. In diesem Fall verläuft die Neuinstallation sehr viel schneller und einfacher, da man nur noch die neueren Patches, die nach der Erstellung des Images publiziert wurden, installieren muss und die Konfiguration des Systems und die Installation der eingesetzten Software schon durchgeführt ist.

Gegenmaßnahmen

Windows 2000 integriert den Windows-Dateischutz *(Windows File Protection – WFP)*, der die vom Setup-Programm installierten Systemdateien im %systemroot% Ordner (normalerweise c:\Winnt) vor dem Überschreiben schützt. Dabei handelt es sich um ungefähr 640 Dateien. Laut neuen Publikationen auf NTBugtraq[30] ist es jedoch bedingt möglich WFP zu umgehen und zu kompromittieren. Als effektive Gegenmaßnahme empfehlen sich Tools wie ‚Tripwire' (http://www.tripwire.com), die Checksummen von allen wichtigen Dateien bilden, bei Veränderungen Alarmmeldungen ausgeben und wahrscheinlich wirkungsvoller sind als WFP.

30http://www.ntbugtraq.com

3.10 Backdoors

Angreifer richten sich gern nach erfolgreichem Zugriff auf ein System eine *Backdoor* (Hintertür) ein, um beim nächsten mal einen leichteren Zugriff zu haben und installieren eventuell noch Tools mit denen sie aus der Ferne Distributed-Denial-of-Service-Angriffe starten können, da diese bei Hackern immer beliebter werden. Deshalb reicht es oft nicht aus, nach der Entdeckung eines Einbruchs nur die Kennwörter zu ändern, da die Backdoors von solchen Maßnahmen nicht an Effizienz verlieren. Die Entdeckung solcher Hintertüren gestaltet sich als nahezu unmöglich, da es fast unendlich viele Wege gibt, Hintertüren zu installieren.

Backdoor-Varianten

Es gibt verschiedene Varianten von Backdoors, von denen hier die meisten beschrieben werden sollen.

1. *Feindliche Benutzerkonten erstellen:* Hiermit sind Benutzerkonten gemeint, denen ein Angreifer wahrscheinlich einen harmlosen Namen gibt, aber sie mit administrativen Rechten versieht. Man sollte also immer die Konten auf unbekannte oder merkwürdige Einträge überprüfen. Es gibt außerdem unter Windows 2000 ein leicht zu benutzendes Tool, um Mitglieder in Gruppen aufzulisten: mit ‚net group' „Administratoren" werden einem die Mitglieder der eingegebenen Gruppe aufgelistet. Auf diese Weise kann man fremde Einträge schnell finden.

2. *Backdoors in Startdateien:* Diese sind sehr beliebt, da arglose Benutzer die Tools bei jedem Neustart wieder starten. Oft installieren Angreifer solche Backdoors, bringen dann den Rechner zum Absturz oder zu einer hohen Systemauslastung, um den Administrator des Systems dazu zu bringen den Rechner neu zu starten und somit ihre Backdoor zu aktivieren. Zu finden sind diese an Einträgen an verschiedenen Stellen im Windows 2000 System. Die Autostart-Ordner im Verzeichnis ‚Dokumente & Einstellungen' der einzelnen Benutzer und der allgemeine Ordner sollten frei von ungewünschten Anwendungen sein. Außerdem gibt es in folgenden Registrierungs-Schlüsseln die Möglichkeit, zu startende Anwendungen unterzubringen:

- HKLM[31]\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AeDebug
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon

Diese können mit der Anwendung ‚regedit.exe' überprüft und Einträge in diesen Bereichen gelöscht werden. Hierbei ist allerdings größte Vorsicht geboten, da schon das unsachgemäße Ändern eines einzelnen Registrierungs-Schlüssels das System unbrauchbar machen kann. Zusätzlich gibt es mit Tools wie ‚DumpReg' von Somarsoft die Möglichkeit, ein Abbild der Registrierung anzufertigen, um zu einem späteren Zeitpunkt einen Vergleich zu machen.

31 HKEY_LOCAL_MACHINE

3. *Zeitgesteuerte Aufgaben:* Es werden Aufrufe in der Warteschlange des Zeitplandienstes eingetragen, die jeden Tag zu einer festen Uhrzeit ausgeführt werden, beispielsweise einen Empfänger auf Port 8080 um 12.00 Uhr einzurichten, über den sich ein Angreifer verbinden kann. Sehen kann man diese Jobs mit dem Befehl ‚at' und das Entfernen ist durch den Aufruf ‚at XYZ /delete' für den unerwünschten Job möglich. Andernfalls kann man mit ‚net stop schedule' den Zeitplandienst stoppen und in der Systemsteuerung unter Dienste das Startverhalten der fraglichen Dienste ändern.

4. *Remote Control:* Ein Angreifer kann ein Tool wie ‚netcat' auf einem System unter anderem Namen speichern, dieses dann auf einem Port auf eine bestimmte Aktion warten lassen und ihn z.B. ‚cmd.exe' ausführen lassen, um den Befehlsinterpreter zu starten. Wenn der Angreifer nun eine Verbindung zu diesem Port aufbaut, wird die Remote-Eingabeaufforderung angezeigt. Für die richtige „Fernbedienung" können Tools wie ‚BackOrifice' oder ‚NetBus' von den Angreifern installiert werden. BackOrifice existiert auch für Windows 2000, heißt ‚BO2k' und ist am Eintrag HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices als Dienst Remote Administration Service in der Registrierung zu erkennen. Mit Tools wie BackOrifice können Rechner grafisch fernbedient werden und Tastatureingaben wie Zugangsdaten aufgezeichnet werden. Alle Remote-Control Tools wie BackOrifice, Netbus oder ‚WinVNC' funktionieren genauso wie unter NT und lassen dadurch große Probleme entstehen.

Gegenmaßnahmen

Momentan stellt schon ein sehr gutes Anti-Viren-Programm einen ausreichenden Schutz dar, da es Trojaner und Backdoors fast immer korrekt erkennt und Warnungen ausgibt, vorausgesetzt man aktualisiert die Virendefinitionen regelmäßig und verwendet die aktuelle Version der Software. Man sollte bei der Auswahl darauf achten, dass das Programm nach Signaturen und Registrierungs-Einträgen suchen kann.

Es ist auch sinnvoll die Protokollierung im Dateisystem zu aktivieren. Im Gegensatz zu Windows NT 4.0 führt bei Windows 2000 diese Einstellung nicht zu exorbitanten Leistungseinbußen, es muss allerdings auch, wie immer beim Logging, jemanden geben, der die Log-Dateien archiviert, um sie vor Veränderungen durch Angreifer, die ihre Spuren verwischen wollen, zu schützen und sie schließlich auch kontrolliert.

Durch die Kontrolle der offenen Ports kann man auch darauf aufmerksam werden, dass Backdoors, die auf dem System nichts zu suchen haben, Ports geöffnet haben. Bei den meisten dieser Tools lassen sich die Ports jedoch ändern, so dass man an den Ports nicht gleich ablesen kann, welche Backdoor installiert wurde. Außerdem kann man diese auch in den Prozesslisten finden. Für dieses Vorgehen muss man sein System gut kennen, um entscheiden zu können, was dort nicht hingehört. Zusätzlich kann man nach bekannten Dateinamen von Backdoors im System suchen, für den Fall, dass der Angreifer sie nicht umbenannt hat.

Für die Remote Control Tools gibt es ein hervorragendes Gegenmittel von Network Flight Recorder namens ‚BackOfficer Friendly'. Es überwacht einige Systemports und meldet Verbindungsversuche. Zusätzlich zeichnet es Benutzernamen und Passwörter, die der Angreifer eingibt, auf. Hat

man die Passwörter, kann man z.B. BackOrifice 2000 problemlos in Server Control mit Shutdown Server und der Option Delete löschen. Das beliebteste Tool der Angreifer ist allerdings ‚VNC' (Virtual Network Computing) von AT&T, da es einem die Macht über das System gibt und kostenlos ist. WinVNC taucht in der Prozessliste auf, ist also sichtbar.

Fazit

Daraus ergibt sich die Konsequenz, dass ein System, das kompromittiert wurde, von den Originalmedien neu installiert werden sollte und danach die Daten vom Backup wieder eingespielt und die aktuellen Patches und Hofixes installiert werden müssen. Nur so kann man von einem erneut sicheren System ausgehen.

Generell bleibt zu sagen, dass man keine Programme ausführen sollte, die man aus dem Internet heruntergeladen hat oder deren Herkunft man nicht sicher einschätzen kann. Oft verbergen sich in harmlos aussehenden Spielen oder kleinen „Helferlein" Trojaner, die dann im Hintergrund völlig andere Dinge tun und großen Schaden anrichten können.

3.11 Tastaturaufzeichnung

Für die Tastaturaufzeichnung werden Tools eingesetzt, die sich zwischen die Tastaturhardware und das Betriebssystem stellen und jede Eingabe in einer versteckten Datei aufzeichnen, auch wenn der Angreifer, der dieses Tool benutzt, um an Benutzernamen und Kennwörter zu gelangen, nicht auf dem Rechner angemeldet ist. D.h. dass der Angreifer nach einer gewissen Zeit wieder auf den Rechner zugreift und die Daten ausliest oder sich diese sogar von einem Trojaner bei einem Verbindungsaufbau über das Internet zuschicken lässt.

Tastaturanschläge lassen sich nach wie vor mit ‚NetBus' oder ‚IKS', dem Invisible Keylogger Stealth, aufzeichnen, die schon bei Windows NT 4.0 ihre Wirkung gezeigt haben. BackOrifice2000 und auch sein Vorgänger haben ebenfalls solche Funktionen integriert.

Gegenmaßnahmen

Als Gegenmaßnahme bietet sich die Suche in der Registrierung nach Werten wie „LogName" an und das Löschen dieser Einträge, wobei man die bereits erwähnte Vorsicht mit Registrierungseinträgen walten lassen sollte.

Mit dem Tool DumpReg von Somarsoft würde man IKS zum Aufzeichnen von Tastaturanschlägen als Treiber im System installiert finden, wenn man ein Abbild der Registrierung angefertigt hat, um zu einem späteren Zeitpunkt einen Vergleich zu machen.

3.12 Webangriffe

Webangriffe zielen direkt auf den Webserver eines Systems. Dieser ist entweder absichtlich aus dem Internet bzw. Intranet erreichbar, wenn es sich um einen öffentlichen bzw. firmeninternen Webserver handelt, oder einfach mit installiert und nie konfiguriert worden. Viele Programme verwenden außerdem inzwischen so genannte *Web-Interfaces*, damit diese über das Web konfiguriert oder verwendet werden können und so die Installation eines Webservers entweder voraussetzen oder selbst vornehmen.
Webangriffe zeichnen sich durch die Verwendung des HTTP-Protokolls aus, das zumindest bei öffentlich erreichbaren Webservern auch durch eine vorhandene Firewall durchgelassen wird, damit der Server genutzt werden kann. Selbst firmeninterne Intranet-Webserver sind häufig gewollt aus dem Internet erreichbar, damit ein Zugriff auf die Daten von außen möglich wird.
Webangriffe können sehr vielseitig sein, reichen vom einfachen Ausspionieren des Netzes bis zur Installation von Backdoors und Trojanern und, weil Webserver häufig Systemdienste sind, haben solche installierten und ausgeführten Programme meistens auch noch besonders hohe Systemrechte.

Ausspionieren von Daten

Webseiten können *Kommentare* enthalten, die normalerweise in einem Browser nicht angezeigt werden. Dennoch überträgt der Webserver die Kommentare und ein Besucher kann sie im *HTML-Code* lesen.
Solche Kommentare können durchaus für einen Angreifer interessante Informationen enthalten. Dazu zählen Adressen von Datenbanken und Hinweise auf Scripte. Programme, die ganze Websites auf bestimmte Kommentare automatisch durchscannen, erleichtern dem Angreifer die Arbeit. Auch die eigentlichen Inhalte einer Website können interessante Informationen enthalten und Telefonnummern oder andere Zugänge verraten.

Unerlaubte Dateizugriffe

Ein Webserver verwaltet seine Dokumente im Dateisystem des Servers. Die Grenze zwischen den öffentlich zugänglichen Internetseiten und den nicht öffentlichen Dateien wird durch das *root-Verzeichnis* des Webservers oder der Website festgelegt. Alle Dateien innerhalb des root-Verzeichnisses sind öffentlich und alle außerhalb nicht. Durch Fehler im Webserver kann diese Grenze durchbrochen werden, so dass der Angreifer auch Zugriff auf Dateien in anderen Verzeichnissen bekommt und diese evtl. auslesen, verändern oder sogar ausführen kann. Da die Position eines root-Verzeichnisses, das ein Webserver nach der Installation verwendet, meist bekannt ist und die Betriebssysteme feste Verzeichnisstrukturen verwenden, können Angreifer gezielt Dateien ansprechen und müssen diese nicht erst suchen.
Das gleiche gilt für Dateien innerhalb der Website, die normalerweise gelesen aber nicht verändert werden dürfen. Da das HTTP-Protokoll auch Schreibzugriffe erlaubt, müssen diese verhindert werden, so dass ein Angreifer nicht in der Lage ist, Dateien zu verändern oder zu erstellen, um die Installation von Programmen oder Scriptdateien zu verhindern.

Script- und Programmcode

Viele Websites enthalten z.B. für Datenbankabfragen Scripte oder CGIs. Dieses werden durch einen Seitenaufruf ausgeführt und stellen dann z.B. Daten aus einer Datenbank in einer HTML-Seite zusammen, um diese an den Besucher zu übertragen.
Normalerweise dürfen solche Programme nicht von einem Besucher gelesen werden. Fehler im Webserver oder in der Konfiguration können dieses jedoch möglich machen, so dass Scriptdateien oder andere Bestandteile heruntergeladen werden können. Ein Angreifer kann in solchen Dateien dann z.B. nach Passwörtern für Datenbankserver suchen und sich so Zugang zu Datenbanken verschaffen. Es können viele wichtige Informationen in solchen Dateien enthalten sein, daher muss das Auslesen unbedingt verhindert werden.

Ausnutzen von Scripten oder Programmen (CGIs)

Die oben erwähnten Scripte und CGIs können natürlich auch Fehler enthalten oder dem Angreifer Funktionen ermöglichen, an die der Entwickler gar nicht gedacht hat. Wie verhält sich z.B. ein Programm, das ein Passwort oder eine E-Mailadresse mit vielleicht 50 Zeichen erwartet und eine Zeichenfolge von mehreren tausend Zeichen bekommt. Werden solche Programme verwendet, um Daten auf den Server zu laden (z.B. für ein Gästebuch), können diese evtl. auch dazu verwendet werden, um bösartigen Programmcode auf den Server zu übertragen. Dieser wird auf dem Server ausgeführt oder in Internetseiten integriert, so dass andere Besucher diesen dann ausführen, wenn sie die Website besuchen.
Programme, die eine Benutzereingabe erlauben, sind von solchen Angriffen immer betroffen. Ein Anmeldeformular nimmt z.B. einen Anmeldenamen entgegen, der dann mit einer Datenbank geprüft wird. Ein Angreifer könnte nun Datenbankbefehle (SQL-Befehle) direkt in das Anmeldeformular schreiben, die dann von dem Datenbankserver ausgeführt werden.

Pufferüberläufe

Pufferüberläufe können in eigenen CGIs, im Webserver oder im System stattfinden und den Server abstürzen lassen oder dazu verwendet werden, Programme auf dem Server auszuführen. Obwohl es sehr kompliziert ist, Pufferüberläufe dazu zu verwenden, sinnvolle Programme auf dem Server auszuführen (siehe Kapitel 3.13) und nur wenige Angreifer in der Lage sind, solchen Angriffscode zu erstellen, bietet das Internet genug Informationen und fertige Programme, mit denen fast jeder in der Lage ist, solche Sicherheitslücken auszunutzen.

Gegenmaßnahmen

Viele Webangriffe können nicht durch eine Firewall geschützt werden, hier muss der Webserver ausreichend eigenen Schutz bieten. Allerdings kann eine Firewall den ausgehenden Verkehr eines Webservers einschränken. Es sollte z.B. von einem Server niemals im Web gesurft werden können, was Firewall bereits verhindern könnte. Würmer, die sich durch Webzugriffe verbreiten, könnten dadurch an der Ausbreitung gehindert werden.
Um sich vor Fehlern im Server zu schützen, die zu Pufferüberläufen führen oder Sicherheitseinstellungen umgehen, hilft nur die Installation von Updates und die regelmäßige Kontrolle von Newslettern, die sich mit diesen Themen befassen. Die Installation eines Betriebssystems von einer CD reicht nicht aus, da diese meist schon veraltet sind. Erst die Installation der aktuellen

Updates kann bekannte Sicherheitsprobleme beheben und vor Fehlern in der Serverprogrammierung und Pufferüberläufen schützen. Um ein System so sicher wie möglich zu machen, können aber noch anderen Maßnahmen getroffen werden.
Damit Daten auf dem Server nicht manipuliert oder unberechtigt gelesen werden, sollten Zugriffsrechte auf einem Webserver genau kontrolliert werden. Ausführbare Dateien, wie CGIs oder Scripte, müssen meist nur ausgeführt werden, das Lesen kann verboten werden.
Internetseiten dürfen keine Kommentare enthalten, die irgendwelche Informationen über das Netzwerk, das Betriebssystem oder andere internen Strukturen verraten.
Die Standardeinstellungen für die Position eines Webverzeichnisses im Dateisystem sollte geändert werden, so dass ein Angreifer sich erst in der Dateistruktur zurechtfinden muss. Wenn möglich, sollten Webverzeichnisse auch nicht im gleichen Dateisystem abgelegt sein, wie das System oder Programme (unter Windows also ein anderes Laufwerk anstelle von Laufwerk C: verwenden).
Alle Daten, die ein Besucher eingeben kann, müssen genau kontrolliert und von bestimmten Zeichen (z.B. „<“ oder „>“) befreit werden, so dass kein bösartiger Code auf den Server übertragen werden kann. Werden diese Daten für Datenbankzugriffe verwendet, muss sichergestellt sein, dass keine Datenbankbefehle übertragen und ausgeführt werden können.
Unnötige Erweiterungen, wie z.B. WebDAV oder Frontpage sollten, wenn man sie nicht verwendet, entfernt werden, da das Deaktivieren solcher Erweiterungen unter Umständen nicht ausreicht. Scriptsprachen, die nicht verwendet werden (z.B. ASP oder Perl) sollte man aus der Konfiguration des Webservers entfernen, damit ein Angreifer keine eigenen Scripte auf dem Server ausführen kann.
Die Überwachung eines Webservers ist besonders wichtig. So können Angriffsversuche erkannt und Gegenmaßnahmen getroffen werden. Obwohl alle Webserver Protokolle erzeugen können, sind diese aufgrund ihrer Größe nicht sehr hilfreich, so dass die Auswertung von einem Programm übernommen werden sollte.

3.13 Pufferüberlauf-Angriffe (Buffer Overflow Error)

Ein *Pufferüberlauf* kann auf verschiedene Weise von einem Angreifer genutzt werden. Besonders gefährlich sind Pufferüberläufe, die über das Netzwerk erzeugt werden können, da ein Angreifer diese leicht verwenden kann und keine fremden Programme auf dem anzugreifenden Computer installieren muss.
Pufferüberläufe basieren auf Fehler in der Programmierung von Computersoftware, obwohl solche Fehler durch sauberes Entwickeln vermieden werden können. Durch die schnelle Entwicklung von Soft- und Hardware verkürzt sich allerdings auch immer mehr die zur Verfügung stehende Entwicklungszeit, so dass Anwender heute mit Produkten arbeiten, die sich noch in der Entwicklungsphase befinden müssten.

Was sind Pufferüberläufe?

Computerprogramme verwenden Unterroutinen, so genannte *Funktionen* oder *Prozeduren*, bzw. *Objekte* und *Methoden* in der *objektorientierten Programmierung*.[32] Ruft ein Programm nun eine Unterroutine auf, so wird für diese ein Speicherbereich reserviert, in dem sie eigene Daten zwischenspeichern kann.
Das Betriebssystem verwendet für diese Speicherbereiche meistens einen Stack, der wie ein Stapel Teller aufgebaut ist. Der letzte Teller (also Speicherbereich), der auf den Stapel gelegt wurde, muss auch zuerst wieder entfernt werden.
Je mehr Routinen sich untereinander aufrufen, desto stärker wächst der Stack im Speicher. Im Idealfall ist der Programmstack am Anfang leer, dann wird die Programmhauptroutine (häufig eine Funktion, die den Namen „main()" trägt) gestartet, die wieder andere Routinen aufruft und den Stack wachsen lassen. Wenn eine Unterroutine beendet wird, wird auch der Speicher im Stack freigegeben und er schrumpft wieder, so dass er im Idealfall beim Programmende wieder leer ist.
Damit das Betriebssystem nach Beendigung einer Unterroutine weiß, wo es das Programm danach im Speicher weiterlaufen lassen soll (nämlich an der Stelle, wo der Aufruf der Unterroutine stattfand), wird diese *Rücksprungadresse* ebenfalls auf dem Stack gespeichert.
Der Stack speichert die Daten, die die Funktionen und Prozeduren jeweils verwenden. Dazu gehören auch Benutzereingaben, wie z.B. Passwörter und Namen, die eine unterschiedliche Länge haben können. Wird im Speicher nur eine feste Speichergröße im Stack für solch eine Eingabe reserviert und diese nicht auf ihre Länge überprüft, kann es passieren, dass wichtige Speicherbereiche im Stack einfach überschrieben werden. Dazu können Teile der Programmroutinen oder auch die Rücksprungadresse gehören.
Dieses Überschreiben wird als Pufferüberlauf bezeichnet und hat meist den Abbruch des betroffenen Programms zur Folge, da das Programm mit sinnlosen Daten überschrieben wurde und das Betriebssystem den Prozess abbricht.. Allerdings kann ein geschickter Angreifer sich dieses Problem zu Nutze machen, indem er nicht sinnlose Daten in den Puffer schreibt, sondern eigenen Programmcode erzeugt und durch Überschreiben der Rücksprungadresse diesen dann ausführen lässt. Da dieser Programmcode direkt in der Sprache des Prozessors geschrieben sein muss, ist er meist sehr effektiv und kann mit wenigen Befehlen sehr viel erreichen, muss allerdings an das Betriebssystem, den Prozessor und die verwendete Software angepasst werden.
Dieser Programmcode wird als Teil des Programms ausgeführt und kann verschiedene Aktionen starten, wie z.B. neue Benutzer anlegen, Dateien oder Programme installieren oder Schaden auf dem Computer anrichten, wenn das eigentliche Programm über genügend Zugriffsrechte verfügt. Sind Programme, wie Webserver, Datenbankserver oder Netzwerksoftware betroffen, verfügen diese meist über sehr hohe Zugriffsrechte im System oder laufen sogar im Speicherbereich des Systems.

---

32 Diese Beschreibung ist nicht für Programmierer gedacht, sie soll den Fehler lediglich illustrieren und ist daher stark vereinfacht.

Um einen Pufferüberlauf dafür zu verwenden, eigenen Programmcode auf einem Computer auszuführen, muss das Betriebssystem und die verwendete Hard- und Software bekannt sein. Außerdem sind gute Programmierkenntnisse und Wissen über das Betriebssystem erforderlich, so dass nur wenige Angreifer solche Programme erzeugen können, da der genaue Zustand des Stacks zum Angriffszeitpunkt bekannt sein muss. Das Internet bietet auch hier genügend Informationen, so dass fast jeder diese Angriffstechnik verwenden kann.

Auswirkungen

Die Auswirkungen eines Pufferüberlaufs sind unterschiedlich und von den Daten abhängig, die den Stack überschreiben. Werden zufällige Daten übergeben, so wird das betreffende Programm wahrscheinlich nur abgebrochen, sind sie jedoch nicht zufällig, sondern wird vom Angreifer Programmcode in den Puffer geschrieben, hängt es davon ab, inwieweit das Programm mit dem Betriebssystem und der Soft- und Hardware des betroffenen Systems kompatibel ist und wie hohe Zugriffsrechte das angegriffene Programm besitzt.
Selbst kleine Programme, die eingeschleust werden, können bereits großen Schaden anrichten und weitere Angriffssoftware aus dem Internet laden und ausführen. Ist dies geschafft, hat der Angreifer eigentlich fast alles erreicht, was er erreichen kann.

Gegenmaßnahmen

Da es sich bei einem Pufferüberlauf um einen Fehler im Programm handelt, kann ein Administrator nur Schadensbegrenzung vornehmen, indem er jegliche Software, die auf einem Computer nicht verwendet wird, entfernt und immer aktuelle Updates der übrigen Software installiert, damit ein erkannter Pufferüberlaufsfehler behoben wird.
Grundsätzlich sollte das System durch Firewalls o.ä. geschützt sein, allerdings nutzt dies wenig, wenn solch ein Fehler in einem Programm vorhanden ist, das absichtlich erreicht werden soll (z.B. Webserver, Fileserver etc.). Wirklich beseitigen können diese Fehler nur die Entwickler, die Programme besser überprüfen müssen, oder Compiler, die Programme erzeugen, die entweder immun gegen solche Fehler sind, oder diese wenigstens erkennen. Entwickler müssen solche Compiler dann auch zur Programmerzeugung verwenden.

4 Sicherheitsprobleme der Komponenten und Gegenmaßnahmen

Durch die vielen neuen Optionen und Konfigurationsmöglichkeiten, von denen die meisten allerdings bei einer Standardinstallation nicht aktiviert sind, ist es fraglich, ob alle Systemadministratoren diese Optionen auch zu nutzen und zu konfigurieren wissen. Allein durch den Fakt, dass Windows 2000 sicherer ist als Windows NT 4.0, sollten sich die Betreiber nicht in Sicherheit wiegen, da es wie bei allen Computersystemen auf die Konfiguration ankommt. Durch die Tatsache, dass Windows 2000 Systeme und auch Server leicht zu installieren sind und dann auch funktionieren, können solche Installationen aber noch lange nicht als sicher bezeichnet werden. Das Heimtückische dabei ist, dass dadurch sehr viele Personen in die Lage versetzt werden solche Systeme aufzusetzen, ohne diese sicher konfigurieren zu können. Wahrscheinlich haben aber gerade deswegen Microsoft Betriebssysteme eine so große Verbreitung. Bei einer guten Konfiguration kann ein Windows 2000 System mindestens genauso sicher sein wie ein UNIX-System oder andere [KUR01].

Ein großes Problem von Windows NT 4.0 war, dass jeder Benutzer in der Registrierung die Schlüssel für Einträge in HKEY_CLASSES_ROOT ändern oder löschen und somit den normalen Betrieb von Anwendungen im System manipulieren konnte. Dieses ist in Windows 2000 nicht mehr möglich, hier kann jeder Benutzer alle Schlüssel einsehen, jedoch nur seine eigenen ändern.

Zwei Sicherheitsprobleme, die gravierend und als ‚getadmin' und ‚sechole' bekannt sind, wurden ebenfalls in Windows 2000 behoben. Man konnte sich mit ihnen unter Windows NT 4.0 in die Gruppe der Administratoren eintragen und so vollen Zugriff auf das System erlangen.

4.1 Sicherheitsrelevante Komponenten

Durch das Hinzufügen vieler Komponenten zu Windows NT 4.0 ist Windows 2000 sicherer geworden, dafür sind unter anderem diese Komponenten verantwortlich:

- IPSec, Internet Protocol Security
- EFS, das verschlüsselnde Dateisystem
- Richtlinienbasierte Sicherheitskonfiguration auf Basis von Gruppenrichtlinien
- Sicherheitsvorlagen, mit denen man Konfigurationen auf allen Rechner angleichen kann
- Integrierte Sicherheitskonfigurations- und –analysetools
- Zentrale Remote Access-Steuerung auf RADIUS-Basis (Remote Access Dial-In User Service)
- Kerberos-Authentifizierung, die das unsichere NTLM ersetzt
- Integriert Public-Key-Verfahren
- Zertifikatsdienste
- Das Active Directory

Im Folgenden werden einige Sicherheitslücken von Windows 2000 aufgedeckt und in den meisten Fällen Gegenmaßnahmen präsentiert.

4.1.1 Windows Inside

Speicherschutzunsicherheit privaten Systemspeichers

Es existiert in Windows 2000 kein Schutzmechanismus für privaten Systemspeicher von im Kernelmodus ausgeführten Komponenten. Daraus folgt, dass Betriebssystem- und Gerätetreibercode, der im Kernelmodus ausgeführt wird, uneingeschränkten Zugriff auf den Systemspeicher hat und die Sicherheitsmechanismen des Speicherschutzes umgehen kann. Da fast der gesamte Windows 2000-Betriebssystemcode im Kernelmodus ausgeführt wird, ist es sehr wichtig, dass andere Software, die im ebenfalls in diesem ausgeführt wird, streng getestet und gut implementiert wurde, um die Systemsicherheit nicht zu gefährden. Dies gilt auch für Gerätetreiber von Fremdherstellern, da diese, sobald sie im Kernelmodus arbeiten, uneingeschränkten Zugriff auf Betriebssystemdaten haben. „Das bedeutet, dass jede Betriebssystemkomponente und jeder Gerätetreiber potenziell Daten beschädigen kann, die von anderen Betriebssystemkomponenten verwendet werden." [SOL00].

Gegenmaßnahmen

Für diese Sicherheitslücke existiert leider keine Gegenmaßnahme, außer sauberer Programmierung in Verbindung mit intensiven Tests seitens der Programmierer von Software, die im Kernelmodus ausgeführt werden muss.

Abgreifen und Injektion von Kennwort-Hash-Sequenzen

Nachdem ein Angreifer das Administratorkonto erobert und sich als Administrator angemeldet hat, ist es laut [KUR01] möglich, die Windows 2000-Kennwort-Hash-Sequenzen abzugreifen, wie es bei Windows NT 4.0 ging. Dieses Vorhaben ist durch die Einführung von SYSKEY etwas schwieriger, aber nicht unmöglich geworden. Man kann mit einer Diskette und NTFSDOS, das zum Lesen von NTFS-Partitionen benutzt werden kann, unter DOS booten, vorausgesetzt das Diskettenlaufwerk ist nicht deaktiviert, und findet dann in ‚%systemroot%\repair' eine Datei, die SAM heißt und das Backup der SAM, in der alle Benutzer stehen, darstellt. Die SAM ist standardmäßig mit SYSKEY verschlüsselt, um sie zu entschlüsseln kann der Angreifer jedoch ‚pwdump2' benutzen, das er allerdings erst auf den Server kopieren muss und für dessen Ausführung er Administratorrechte braucht.
Ein weiteres Problem in diesem Rahmen ist die Injektion von Hashsequenzen in die SAM, die funktioniert, obwohl die SAM mit SYSKEY verschlüsselt wird, da der Rechner die Hashsequenzen nach einem Neustart einfügt. Petter Nordahl-Hagen hat eine Linux-Bootdiskette entwickelt, mit der man ein Windows 2000 System booten und das Administratorkennwort ändern kann, indem SYSKEY deaktiviert wird, sogar wenn der Administrator umbenannt wurde, da das Tool mit der RID 500 des Administrators arbeitet, die man nicht verändern kann. Herunterladen kann man das Diskettenimage unter http://home.eunet.no/~pnordahl/ntpasswd und wir können die Funktionalität bestätigen. Unter [URL23] und [URL24] sind die Beschreibungen hierzu enthalten. Bei falscher Vorgehensweise der beigelegten Tools ist es allerdings schon oft vorgekommen, dass ein System unbrauchbar wurde und neu installiert werden musste, wobei es natürlich zum Datenverlust kommt, wenn man kein intaktes Backup besitzt. Dieses funktioniert nicht auf Domänencontrollern, da die Benutzerinformationen im Active Directory gespeichert sind und dieses Vorgehen nur bei der SAM funktioniert.

Gegenmaßnahmen

Die angemessene Gegenmaßnahme, wenn man solche Angriffe befürchtet, ist das Sichern von SYSKEY und die Aktivierung der Option, den Schlüssel von einer Diskette beim Booten zu verlangen oder ein extra Passwort anzufordern. Falls die Diskette nach häufiger Benutzung Fehler aufweist und man keine Kopie bereit hält, hat man allerdings ein großes Problem. Die Einstellung nimmt man vor, indem man ‚syskey.exe' startet, dort auf Aktualisieren klickt und die gewünschte Option einstellt.

Verstecken von Daten

Wenn Angreifer ihre Tools auf ein System gebracht haben, wollen sie diese meist umbenennen und verstecken. Das geht nach wie vor mit dem ‚attrib' Befehl, der es ermöglicht, das Dateiattribut einer Datei auf *hidden* zu setzen. Auch mit NTFS 5 gibt es außerdem die Möglichkeit, Dateien in Datenströmen hinter anderen Dateien, und somit in einer Datei, zu verstecken.

Gegenmaßnahmen

Dateien, die versteckt sind, sind im Windows-Explorer allerdings sichtbar, wenn die Option ‚Alle Dateien und Ordner anzeigen' in Extras, Ordneroptionen unter Ansicht gewählt ist. Bei Dateien in Dateiströmen wird es mit Windows-Bordmitteln schwierig, diese zu finden. Bei Kopiervorgängen von Dateien von NTFS-Datenträgern auf FAT- Datenträger, die keine Dateiströme unterstützen, wird beim Kopiervorgang einer Datei mit mehreren Dateiströmen eine Warnmeldung ausgegeben. Solche Dateien kann man allerdings auch mit Tools von Fremdherstellern finden. ‚sfind' von NTObjectives aus deren Forensic Toolkit gehört zu dieser Gruppe.

Löschen der Protokolle

Zum Verwischen der Spuren haben die Angreifer zum größten Teil noch die Tools, die sie bei Windows NT 4.0 benutzt haben, und sie sind noch funktionsfähig. Es ist also möglich, die Protokollierung zu deaktivieren und es wird, nicht wie bei UNIX, nichts weiterprotokolliert. Hat ein Angreifer sich als Administrator angemeldet, kann er mit dem aus Windows NT 4.0 bekannten ‚elsave' Utility die Ereignisprotokolle löschen und auf diese Weise seine Spuren verwischen. Es gibt keine Möglichkeit dies rückgängig zu machen.

Gegenmaßnahmen

Gegen dieses Problem kann man nichts tun, außer seine Protokolldateien regelmäßig auszulagern, um sie später mit den noch vorhandenen zu vergleichen und so auf Manipulationen zu stoßen oder in den archivierten Dateien Hinweise auf Angriffe zu finden.

Angreifbarkeit Lokaler Prozeduraufrufe (LPCs)

Es gibt einen Bug laut *Microsoft Security Bulletin MS 00-070*, der bewirkt, dass LPCs angreifbar sind. Mit einem Angriff kann der Speicher aufgebraucht, ein Denial-of-Service-Angriff durchgeführt oder Code im Sicherheitskontext des angemeldeten Benutzers ausgeführt werden. Dafür muss der Angreifer allerdings lokal angemeldet sein.

Es existiert ein Hotfix, der das Problem behebt und nicht in Service Pack1, aber in Service Pack 2 enthalten ist.

Angreifbarkeit von Remote Prozeduraufrufen (RPCs)

Ein Bug in Windows 2000 ermöglicht laut *Microsoft Security Bulletin MS 00-066,* dass ein Angreifer durch das Senden eines speziell missgeformten RPC-Pakets den RPC-Service zum Absturz bringen und damit einen DoS-Agriff durchführen kann. Dieser Angriff funktioniert nur bei Rechnern auf denen die Ports 135 bis 139 und 445 aktiv sind.

Gegenmaßnahmen

Microsoft stellt einen Hotfix bereit, der nicht in Service Pack 1, aber in Service Pack 2 enthalten ist und das Problem behebt. Man kann außerdem, wenn man NetBIOS nicht benötigt, die Ports 135-139 und 445 deaktivieren und damit viele Sicherheitslücken schließen.

Weitere Angreifbarkeit von Remote Prozeduraufrufen (RPCs)

Ein Fehler in der Windows 2000-RPC-Implementation ermöglicht laut *Microsoft Security Bulletin MS 01-041,* einen Angriff auf das System. Hierfür muss ein Angreifer speziell missgeformte Daten an den RPC-Dienst senden und dies läuft, da der RPC viele Eingaben nicht überprüft und sie demnach ausführt, auf einen Denial-of-Service-Angriff hinaus, der von zeitweiliger Unerreichbarkeit bis zum Ausfall des RPC-Dienst führen und einen Neustart erfordern kann.

Gegenmaßnahmen

Es ist ein Patch bei Microsoft erhältlich, der das Problem behebt, indem er eine Überprüfungsroutine in den RPC-Dienst einbindet und diese ab sofort die Eingaben kontrolliert. Der Patch ist nicht in Service Pack 1 und 2 enthalten, soll aber Bestandteil von Service Pack 3 sein.

Ausnutzung vorhersagbarer NamedPipes

Durch einen Fehler, der im *Microsoft Security Bulletin MS 00-053* beschrieben wird, ist es für einen lokal angemeldeten Benutzer, der sich z.B. über den Terminal Server angemeldet hat, möglich, Code mit Systemberechtigung auszuführen, um damit beispielsweise den eigenen Benutzer zur Gruppe der Administratoren hinzuzufügen und somit selbst zum Administrator zu werden. Hierzu werden NamedPipes vorausgesagt und mit ihnen die Rechte für einen zu startenden Prozess, so dass mit diesem die Rechte des angemeldeten Benutzers erweitert oder beliebiger Code mit Systemberechtigung ausgeführt werden kann. Man kann die nächste NamedPipe durch Einträge in der Registrierung unter HKLM\System\CurrentControlSet\Control\ServiceCurrent auslesen und diese instanziieren, um Code im Sicherheitskontext von SYSTEM auszuführen. Beliebiger Code, der an der NamedPipe hängt, wird dann mit Systemberechtigung ausgeführt.

Gegenmaßnahmen

Bei Microsoft kann man einen Hotfix erhalten, der diese Sicherheitslücke behebt und nicht zum Service Pack 1 gehört. Dieser muss alleine installiert werden.

Probleme durch den relativen Shell-Pfad

Der relative Shell-Pfad ermöglicht, dass ein Angreifer eine auszuführende Datei in einem Verzeichnis speichert, das in der Startreihenfolge vor dem Verzeichnis der Originaldatei durchsucht wird. Somit wird die Datei des Angreifers ausgeführt. Im *Microsoft Security Bulletin MS00-052* wird dieser Bug beschrieben. Da Windows beim Systemstart viele Programme, wie beispielsweise

seine Shell, lädt und diese im ganzen System ausgehend vom Root-Verzeichnis gesucht werden, ist es für einen Angreifer ein leichtes, einen Trojaner mit dem Namen ‚explorer.exe' in das Root-Verzeichnis zu kopieren und ihn dann automatisch starten zu lassen. Man kann sogar mit Tools wie ‚eLiTeWrap' Code an andere Dateien wie die ‚explorer.exe' anhängen und diesen dann mitausführen lassen. Diese Sicherheitslücke hat schon BackOrifice ausgenutzt, ohne dass die Benutzer etwas davon mitbekommen haben. Das Verfahren funktioniert auch für DLLs und man kann sich über den Telnet-Server, falls dieser aktiv ist, was über TCP Port 3389 herauszufinden ist, auf dem System anmelden und per FTP seine Dateien dort hin kopieren, um sie ausführen zu lassen.

Gegenmaßnahmen

Hierfür gibt es einen Patch von Microsoft, der nicht im Service Pack 1 enthalten ist. Durch ihn wird der Startup Code geändert, indem der %systemroot%-Pfad der Shell vorangestellt wird. Somit werden die Anwendungen, die beim Start im %systemroot% liegen, zuerst ausgeführt. Trotzdem kann natürlich ein Angreifer diese Dateien verändern oder an Code anhängen, der dann mitausgeführt wird. Diese Angriffsform erfordert sehr hohe Wachsamkeit bei den Systemadministratoren, da sie schwer zu bemerken ist.

Umgebungsvariablenpufferüberlauf

Die Anwendung ‚cmd.exe', der *command processor*, hat laut [KUR01] einen Fehler im Codeteil für die Umgebungsvariablen und ein Angreifer könnte damit einen extrem langen Umgebungsvariablenstring erzeugen, der einen Pufferüberlauf erzeugt. Dies führt zum Absturz des Prozesses und der Speicherbereich des Prozesses kann nur durch das Anklicken eines nach dem Absturz auftauchenden Eingabefensters freigegeben werden. Handelt es sich bei dem Ziel um einen unbeaufsichtigten Server, können durch nicht wieder freigegebenen Speicher sämtliche Systemressourcen aufgebraucht werden.

Gegenmaßnahmen

Ein Hotfix hierfür ist auf den Microsoft-Internetseiten erhätlich.

Winstation-Zugriffsverletzung

Dem *Microsoft Security Bulletin MS 00-020* zu Folge ist ein Bug in der Implementierung von Windows Stations (Winstation) vorhanden. Basierend auf der Hierarchie Sitzung, Winstation, Desktop, bei der es in jeder Sitzung eine oder mehrere Windows Stations (Winstations) gibt und in diesen mehrere Desktops existieren können, wurde laut Implementierung festgelegt, dass Prozesse in einer Winstation ablaufen und nicht auf andere zugreifen können. Durch einen Programmierfehler könnte es sein, dass Benutzer von anderen Benutzern input- oder output-strings auf Desktopebene abfangen können, und so beispielsweise an Passwörter herankommen könnten. Dies gilt nur für lokal angemeldete Benutzer. Außerdem kann ein Benutzer eines Rechners unter Umständen seine Rechte ausbauen und Informationen von anderen Benutzern sehen.

Gegenmaßnahmen

Diese Sicherheitslücke wurde durch einen Patch in Service Pack 1 geschlossen, er ist aber auch einzeln erhältlich. Es bleibt zu hoffen, dass nicht noch weitere Fehler in Winstation enthalten sind, die solch gravierende Lücken eröffnen.

4.1.2 Access Control

Administrator hat Zugriff auf alle Dateien

Besitzer von Objekten haben immer Schreibzugriff auf die DACL. Wenn sie leer ist, kann der Besitzer eine neue DACL mit den gewünschten Rechten einrichten und das Objekt damit in Besitz nehmen. Aus dieser Konstellation ergibt sich eine Sicherheitslücke, da für den Fall, dass ein Benutzer dem Administrator den Zugriff zu einem Objekt explizit verweigert, der Administrator mit seinen Rechten trotzdem den Besitzer des Objektes ändern und sich selbst eintragen kann. Damit hat er wieder Zugriff auf das Objekt. Der Administrator kann folglich immer auf alle Objekte zugreifen.

Gegenmaßnahmen

Diese Sicherheitslücke kann in Windows 2000 nicht geschlossen werden.

Umgehung der Zugriffsbeschränkung für Dateien durch eine Bootdisk

Durch das Booten mit einer Startdiskette, die ein Programm zum Lesen von NTFS-Partitionen enthalt, ist es möglich, die Dateien auf den Festplatten-Partitionen einzusehen, ohne die Rechte für diese Dateien zu besitzen, falls sie nicht mit dem verschlüsselnden Dateisystem (EFS) geschützt worden sind.

Gegenmaßnahmen

Aus diesem Grund sollten Diskettenlaufwerke im Bios deaktiviert werden, außer man hat den zum Start benötigten Schlüssel auf Diskette ausgelagert. Außerdem empfiehlt sich der Einsatz des verschlüsselnden Dateisystems und zusätzlich das Auslagern des Schlüssels für den Wiederherstellungsagenten, damit man die verschlüsselten Dateien bei Eroberung des Wiederherstellungsagentenkontos nicht entschlüsseln kann.

Umgehung der Zugriffsbeschränkung für Dateien durch Ausbau der Platte

Eine weitere Möglichkeit ist das Ausbauen der Festplatte und der Einbau in ein anderes Windows 2000 System, bei dem ein als Administrator angemeldeter Benutzer den Inhalt der Platte ohne Einschränkungen lesen kann und somit wie bei dem vorherigen Beispiel die Zugriffskontrolle wirkungslos ist.

Gegenmaßnahmen

Auch dies wird vom verschlüsselnden Dateisystem verhindert. Zusätzliche Sicherheit bietet der Einsatz von SYSKEY mit der Option Passwort oder der Auslagerung des Start-Schlüssels auf eine Diskette. Auch hier empfiehlt sich die Auslagerung des Wiederherstellungsagentenschlüssels.

Ändern von Benutzerpasswörtern mit ‚chntpw'

Mit einem Tool namens ‚chntpw' kann man das Passwort eines Benutzers ändern, um sich dann selbst als dieser anzumelden und z.B. seine in EFS verschlüsselten Daten einsehen zu können. Dies funktioniert genauso wie bereits unter Windows NT 4.0 [KUR01].

Gegenmaßnahmen

Gegen ‚chntpw' gibt es nach unserer Erkenntnis keine Gegenmaßnahmen.

Aufhebung der Sperrung von Benutzerkonten nach falscher Anmeldung

Laut *Microsoft Security Bulletin MS00-89* gibt es einen Bug, der es ermöglicht, die Sperrung eines Benutzerkontos nach mehrmaliger falscher Eingabe des Passworts zu deaktivieren, obwohl dies in den Sicherheitsrichtlinien eindeutig so konfiguriert ist, und damit Brute-Force-Angriffe auf Konten zu ermöglichen, indem die Einstellungen des Administrators in diesem Bereich deaktiviert werden. Die Sicherheitslücke betrifft nur Windows 2000 Rechner, die nicht in einer Domäne betrieben werden und somit den NTLM zur Anmeldung verwenden.

Gegenmaßnahmen

Es gibt einen Hotfix auf den Microsoft-Internetseiten, der nicht in Service Pack1, aber in Service Pack 2 enthalten ist.

Räumlicher Zugriff

Zusätzlich zur Sicherung des Betriebssystems sollte selbstverständlich eine räumliche Zugangssicherung vorhanden sein. Dies gilt für jedes sicherheitsrelevante Computersystem, bei dem beispielsweise der Zugang zu der EDV-Abteilung nur den wichtigsten Personen vorbehalten sein sollte.

Gegenmaßnahmen

Eine Sicherung per Magnetkartenauthentifizierung oder funktionierendem Biometrik-Scan können hier die Sicherheit wesentlich erhöhen, aber auch eine abgeschlossene Abteilung mit Zahlenschloß oder Schlüssel reicht aus, um nicht alle Mitarbeiter in Abteilungen gehen zu lassen, die nicht zu ihrem Zuständigkeitsbereich gehören.

Social Engineering

Nicht unerwähnt bleiben soll natürlich auch die systemunabhängige Methode des Manipulierens von Personen. Ein Angreifer ruft beispielsweise einen Mitarbeiter über seine, auf der Internetseite des Unternehmens erhältliche, Durchwahl an, gibt sich mit einem erfundenen Namen für den neuen Systemadministrator aus und fragt nach Benutzernamen, Passwort und seinem Betriebssystem oder Anmeldeclient. Somit hat er genug Informationen, um einen erfolgreichen Angriff zu starten, für die er normalerweise viel Arbeit hätte investieren müssen, oder sie gar nicht erlangt hätte.

Gegenmaßnahmen

Um solche Probleme zu verhindern, muss man seine Mitarbeiter über solch allgemeine und auch akute Sicherheitsprobleme regelmäßig aufklären und deren Wachsamkeit für diese wecken. Außerdem sollte es Vorgehensweisen für die Systemadministratoren und das Wartungspersonal geben, die eindeutig sind und die externe Angreifer nicht erraten können. Dabei müssen natürlich auch die Mitarbeiter auf die Ausführung dieser Methoden bestehen. Den Mitarbeitern muss eingeprägt werden, dass es solche Sicherheitsprobleme gibt und sie mithelfen müssen, die Sicherheit aufrecht zu erhalten.

4.1.3 Active Directory

Windows 2000 verwendet das Active Directory als Verzeichnisdienst und Datenspeicher. Einige Windows 2000 Dienste und andere Programme verwenden das Active Directory zur Speicherung ihrer Konfiguration. Die Unterscheidung zwischen dem Active Directory und der Registrierung in einigen Beschreibungen ist oft nicht sehr präzise, generell ist das Active Directory aber getrennt von dieser zu betrachten und es verwendet auch eine eigene Datenbank, die sich normalerweise im Ordner „NTDS“ im Systemverzeichnis befindet, der Ort kann während der Installation aber auch geändert werden.
Genau wie die Objekte in der Registrierung wird auch jedes Active Directory Objekt durch DACLs geschützt, so dass die Zugangsberechtigungen für jedes Objekt getrennt festgelegt werden können.

Zugriff auf das Active Directory

Auf das Active Directory kann mit dem LDAP Protokoll über das Netzwerk zugegriffen werden. Außerdem ist der Zugriff durch Programme über eine API möglich und für den Benutzer über diverse Verwaltungsprogramme. Es erscheint in Hinsicht auf die vielen Zugriffsmöglichkeiten wichtig, die Zugangsberechtigungen und Zugriffsrechte für enthaltene Objekte sorgfältig zu treffen.
In diesem Zusammenhang gibt es zwei Betriebsarten des Active Directory, die den Zugriff für NT 4.0 Domänencontroller steuern. Es kann ein Windows 2000 Domänencontroller die Rolle eines primären Domänencontrollers (PDC) für NT 4.0 Server übernehmen, so dass auch die Backup Domänen Controller (BDC) von NT 4.0 verwendet werden können. Der Windows 2000 PDC regelt dann den Zugriff auf die Daten im Active Directory. Eine Umstellung in den einheitlichen Windows 2000 Modus ist jederzeit möglich, zurück gibt es allerdings keinen Weg.
In diesem Zusammenhang ist auch die Gruppe „Prä Windows 2000 kompatibler Zugriff“ wichtig. Ist die Gruppe „Jeder“ Mitglied dieser Gruppe, können anonyme Benutzer auf das Active Directory zugreifen und über LDAP oder NetBIOS-Null-Sessions anmelden und Informationen aus der Domäne auslesen.

Ausspionieren von Daten aus dem AD

Das Active Directory enthält viele für einen Angreifer interessante Informationen und ist unter Umständen ähnlich zugriffsfreundlich wie die NetBIOS-Null-Session. Windows 2000 Domänen speichern alle wichtigen Daten im Active Directory, wozu auch Benutzerkonten, Informationen über Computer, Drucker und andere Objekte gehören. Diese Informationen sind für einen Angreifer äußert hilfreich und dürfen auf keinen Fall veröffentlich werden.

Gefahren

Die erbeuteten Informationen dienen dem Angreifer erst einmal dazu, sich ein Bild von der Infrastruktur des Netzwerkes zu machen. Da sich Informationen über die Benutzer, Computer und Standorte im AD befinden, kann er das fremde Netzwerk gut rekonstruieren und diese Informationen für das weitere Vorgehen nutzen.

Gegenmaßnahmen

Zuerst sollte der Zugriff auf das Active Directory weitestgehend eingeschränkt werden. Protokolle wie LDAP oder NetBIOS sollten durch eine Firewall blockiert werden, wodurch zunächst nur der Angriff von außen verhindert werden kann.
Sind keine NT 4.0 Domänencontroller im Netzwerk vorhanden, kann das Active Directory in den *einheitlichen Modus* versetzt werden. Dazu wird das Verwaltungprogramm ‚Active Directory-Benutzer und -Computer' aufgerufen. In den allgemeinen Eigenschaften einer Domäne kann diese in den einheitlichen Modus versetzt werden. (Achtung, es gibt keinen Weg zurück!)

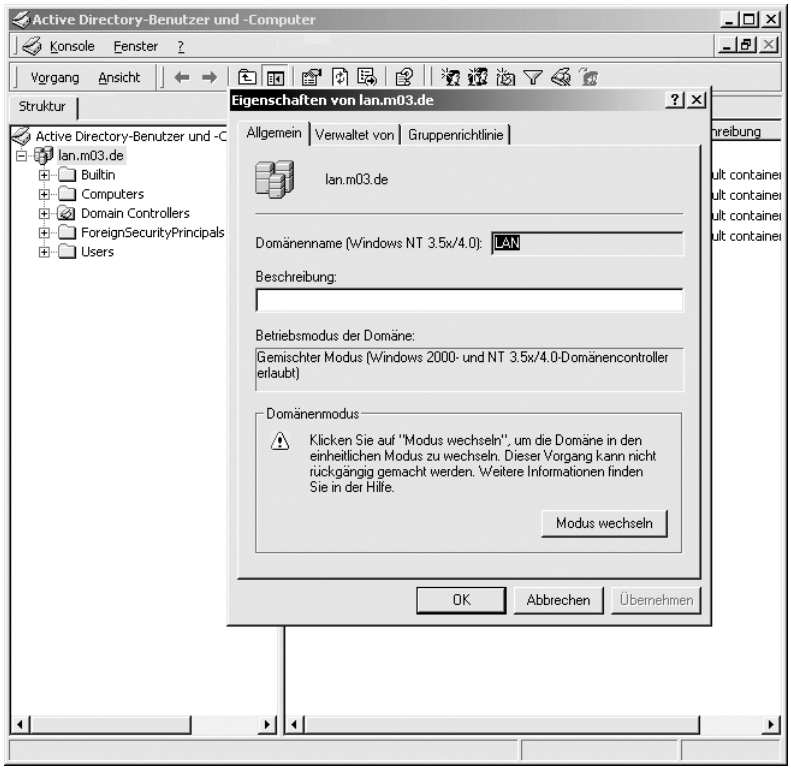

Abbildung 4-1 Aktivieren des einheitlichen Modus

Außerdem sollte die Gruppe „Jeder" aus der „Prä Windows 2000 kompatibler Zugriff"-Gruppe entfernt werden, damit keine anonymen Anmeldungen an das AD möglich sind. Auch dafür wird das Verwaltungsprogramm ‚Active Directory-Benutzer und -Computer' verwendet.

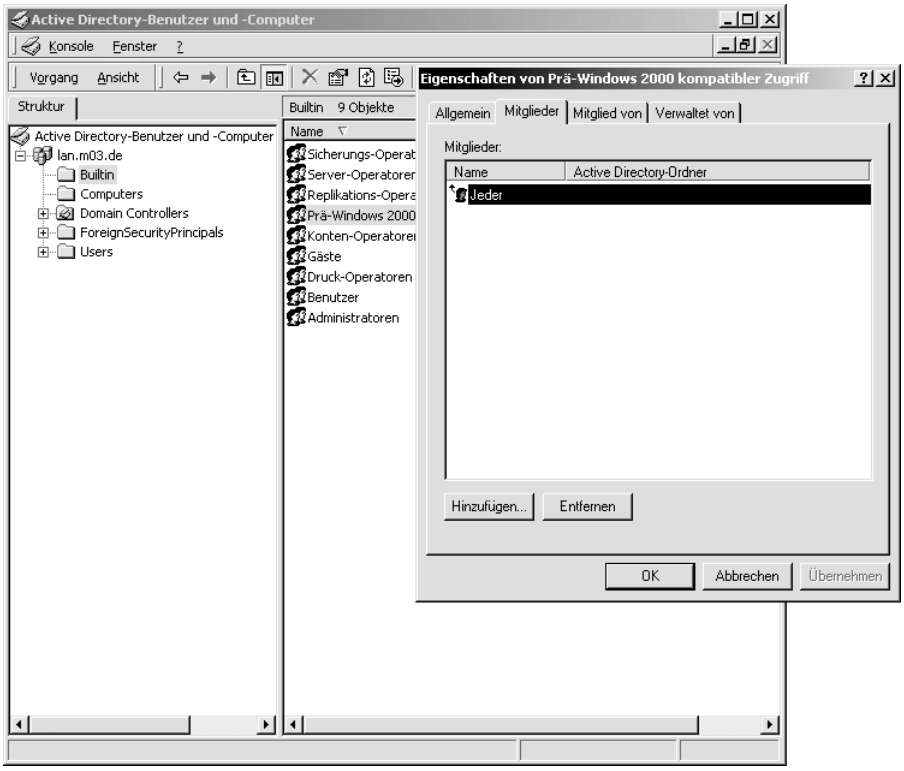

Abbildung 4-2 Entfernen der Gruppe „Jeder" aus der Gruppe „Prä-Windows 2000 kompatibler Zugriff"

Bekannte Sicherheitsprobleme

Das Microsoft Security Bulletin Dokument MS01-036 beschreibt einen Fehler, der es einem Angreifer ermöglicht, bestimmte Daten per LDAP im Active Directory zu verändern. Das Problem ist, dass es sich bei den bestimmten Daten um Benutzerpasswörter handelt. D.h., ein Angreifer kann z.B. das Passwort von einem Domänen-Administrator verändern und das Benutzerkonto dann selbst verwenden.
Dieser Fehler tritt nur auf, wenn der Zugriff über LDAP mit SSL verschlüsselt wird, da eine fehlerhafte Routine dann die Zugriffsrechte für die Objekte im Active Directory nicht korrekt überprüft. Jeder, der LDAP mit SSL einsetzt, sollte sofort das Softwareupdate installieren, um diese gefährliche Sicherheitslücke zu schließen.

Replikation der AD-Daten

Die Daten im Active Directory werden durch die Server repliziert. Diese Replikation kann im lokalen Netzwerk zwischen zwei Domänencontrollern oder zwei Standorten über öffentliche Netze stattfinden.
Die Server verwenden zwei Techniken für die Replikation der Active Directory-Daten. Die erste Methode wird IP-Replikation genannt und verwendet Remote Procedure Calls (RPCs), um die Daten über das Netzwerk zu transportieren. Diese Methode kann sowohl im lokalen Netzwerk als auch zwischen Standorten verwendet werden. Die zweite Methode verwendet das SMTP-Protokoll zur Übertragung der Daten und wird SMTP-Replikation genannt. Diese Methode wird nur zwischen zwei Standorten verwendet und benötigt eine Zertifizierungsstelle, um die Daten verschlüsseln zu können. Durch die Verwendung des SMTP-Protokolls, kann diese Methode auch durch Firewalls eingesetzt werden.

Gefahren

Die Übertragung solch wichtiger Daten über öffentliche Netze ist nicht ungefährlich, ebenso kann die interne Replikation unter Umständen durch interne Angreifer gefährdet werden. Sollte ein Angreifer in der Lage sein, die Daten während der Replikation zu verändern oder die Replikation anderweitig zu beeinflussen, wäre er in der Lage wichtige, Daten im System zu ändern.

Gegenmaßnahmen

Obwohl keine Sicherheitsprobleme zu diesem Thema bekannt sind, ist es ratsam, die Verbindungen zwischen den Standorten zu sichern und verschlüsselte Übertragungswege zu verwenden. Protokolle, wie IPSec und sichere IP-Tunnel, verschlüsseln die Daten zuverlässig und sorgen für eine fehlerfreie Übertragung.

Auslesen von Passwort-Hash-Sequenzen

Windows 2000 speichert seine Benutzerkonten auf Domänencontrollern im Active Directory. Dort werden auch die Hash-Werte der Passwörter gespeichert. Im Gegensatz zur SAM-Datenbank ist es hier schwieriger an die Hash-Werte heranzukommen, aber nicht unmöglich. Es gibt ein Programm ‚pwdump2', das in der Lage ist, die Hash-Werte aus dem Active Directory auszulesen und eine Entschlüsselung dann ermöglicht. Zur Zeit muss das Programm, das von Todd Sabin entwickelt wurde, noch mit administrativen Rechten lokal auf dem Server ausgeführt werden. [KUR01]

Gefahren

Hat ein Angreifer die Hash-Werte der Passwörter, ist es nur eine Frage der Zeit bis diese entschlüsselt sind. Je nach verwendetem Passwort kann die Entschlüsselung einige Minuten oder mehrere Tage dauern.

Gegenmaßnahmen

Da momentan das Programm noch lokal am Rechner mit einem administrativen Konto ausgeführt werden muss, kann ein Angreifer es nur dann starten, wenn ein Administrator sich am Server nicht abgemeldet hat. Genau das sollte ein Benutzer am Server immer tun, wenn er diesen verlässt. Auch die Verwendung von sicheren Passwörtern kann nicht häufig genug erwähnt werden, da ein Angreifer sonst die Passwörter schnell entschlüsseln oder vielleicht sogar erraten kann.

4.1.4 Encrypting File System (EFS)

Privater EFS-Schlüssel ist auf der Festplatte gespeichert

In Windows 2000 werden die privaten Schlüssel für die Entschlüsselung auf der Festplatte des Computers gespeichert. Daraus ergibt sich eine große Sicherheitslücke und sie soll erst in zukünftigen Betriebssystemversionen dahingehend behoben werden, dass Schlüssel auf portablen Medien wie Smartcards gespeichert werden sollen.

Gegenmaßnahmen

Es gibt keine Gegenmaßnahmen, da man diese Schlüssel nicht auslagern kann.

Verschlüsselung geht beim Kopieren auf nicht NTFS-Datenträger verloren

Wird eine mit EFS verschlüsselte Datei von einer NTFS5-Partition auf eine nicht NTFS5-Partition kopiert, wird die Datei im Hintergrund von EFS entschlüsselt und im Klartext auf der Zielpartition gespeichert. Bei Kopiervorgängen auf einen Datenträger, der nicht NTFS5 formatiert ist, egal ob im Windows Explorer oder der Eingabeaufforderung, geht die Verschlüsselung auf dem Zieldatenträger verloren. Hierzu zählen viele Medien, die für den Datenaustausch benutzt werden. Außerdem erscheint auch keine Warnmeldung, dass die Datei nach dem Kopieren nicht mehr verschlüsselt ist.

Gegenmaßnahmen

Gegen dieses Problem gibt es keine Maßnahme.

Administrator kann verschlüsselte Dateien lesen

Der Administrator kann auf einem Windows 2000 System alle Dateien sehen, da er standardmäßig der Wiederherstellungsagent (Key-Recovery-Agent - RA) ist. Für den Fall, dass der Wiederherstellungsagent ein anderer Benutzer ist, gibt es Tools, um sein Passwort zurückzusetzen und das Konto dann benutzen zu können. Durch das Löschen des Wiederherstellungsagenten kann dies auch nicht unterbunden werden, da dann das EFS nicht mehr funktioniert, weil es seine Existenz vorschreibt. Daten, die vorher verschlüsselt wurden, kann in diesem Fall nur der Benutzer, der sie verschlüsselt hat, wieder öffnen. Ist der Rechner Mitglied einer Domäne, werden die Zertifikate und Schlüssel auf den Domänencontroller kopiert und der Domänenadministrator wird zum Wiederherstellungsagenten. Gleichzeitig ist der Administrator nicht mehr der Wiederherstellungsagent auf dem lokalen Rechner, was Angreifern diesen Zugriff extrem erschwert. Trotzdem sollte man das Zertifikat des Wiederherstellungsagenten exportieren und sichern, da der Domänencontroller gelöscht werden könnte und man dann das Zertifikat braucht.

Gegenmaßnahmen

Als Gegenmaßnahme empfiehlt sich der Export des Wiederherstellungsagentenschlüssels, indem man unter Verwaltung, lokale Sicherheitsrichtlinie, Richtlinien öffentlicher Schlüssel, Agenten für Wiederherstellung von verschlüsselten Daten mit der rechten Maustaste anklickt, Alle Aufgaben-Exportieren und dann beim Export Privaten Schlüssel nach erfolgreichem Export löschen wählt, dieser Export ist entscheidend für die Sicherheit. Bei dem Vorhandensein einer Domäne werden alle Wiederherstellungsagenten auf den Workstations deaktiviert und ihr Schlüssel beim Wiederherstellungsagenten auf dem Domänencontroller abgelegt. Auch diesen sollte man der Sicherheit halber exportieren, da dann nicht einmal bei der Eroberung des Domänencontrollers durch einen Angreifer die Verschlüsselung von Daten aufgehoben werden kann, es sei denn er kann sich als ihr Besitzer anmelden. Ganz besonders bei tragbaren Computern wird die Sicherheit durch das Löschen des privaten Schlüssel des Wiederherstellungsagenten sehr erhöht.

Verschlüsselung geht durch nicht angepasste Backup-Programme verloren

Nur Windows 2000 kompatible Backup-Programme können verschlüsselte Daten so sichern, wie sie vorliegen, bei allen anderen geht die Verschlüsselung beim Kopiervorgang auf das Sicherungsmedium verloren. Das integrierte Backup-Programm von Windows 2000 kann die Dateien

richtig sichern, es bietet aber keinen großen Funktionsumfang, so dass die meisten Anwender auf Produkte von Fremdherstellern ausweichen werden und diese vor dem Kauf gut inspizieren sollten.

Gegenmaßnahmen

Außer der Verwendung Windows 2000-konformer Backup-Programme gibt es keine Gegenmaßnahmen.

Verschlüsselte Dateien sind von anderen Benutzern löschbar

Andere Benutzer, die Zugriff auf die Verzeichnisse des Benutzers haben, der Dateien verschlüsselt hat, können die Dateien zwar nicht lesen oder ändern, sie können sie aber löschen.

Gegenmaßnahmen

Man kann die Zugriffsrechte für die verschlüsselten Dateien ändern, so dass man nur noch selbst Zugriff darauf hat, damit ist allerdings der Administrator nicht ausgeschlossen. Bei Verzeichnissen auf einem Server, den mehrere Benutzer oder gar Benutzergruppen benutzen, könnte dies allerdings schwierig werden.

Probleme durch Verschlüsselung von Systemdateien

Normalerweise dürfen Benutzer, auch Administratoren, keine Dateien im Root- und Systemverzeichnis verschlüsseln. Bei einem solchen Versuch erscheint sofort eine Warnmeldung. Unter bestimmten Voraussetzungen, beispielsweise mit dem Befehlszeilentool ‚cipher.exe' für EFS, ist es Administratoren jedoch möglich, Dateien im Systemordner zu verschlüsseln. Dies ist allerdings fatal, weil diese beim Systemstart nicht geladen werden können, da der Benutzerschlüssel zum Entschlüsseln, und somit das ganze verschlüsselnde Dateisystem, während des Startvorgangs nicht zur Verfügung steht. Werden dennoch Systemdateien verschlüsselt, kann das System unbrauchbar werden. Der Windows Explorer warnt bei solch einem Vorgehen, zukünftige Windows Versionen sollen das Verschlüsseln von Systemdateien unterstützen.

Gegenmaßnahmen

Unter normalen Umständen können Systemdateien nicht verschlüsselt werden und zusätzlich werden Warnmeldungen generiert. Das mutwillige Verschlüsseln durch den Administrator unter gewissen Voraussetzungen kann allerdings nicht verhindert werden.

Verschlüsselte Dateien werden unverschlüsselt übertragen

Eine große Sicherheitslücke von EFS besteht darin, dass die Daten während ihrer Übertragung im Netzwerk im Klartext übertragen werden. Wird eine Datei auf einem Server geöffnet, so ist zu bedenken, dass die Übertragung der Datei(en) unverschlüsselt passiert und sie somit abgehört werden können. Genauso ist es beim Speichern auf einem Server und beim Kopieren einer verschlüsselten Datei auf einen anderen Server mit NTFS5 oder von einem Server zu einem anderen. Dabei wird die Datei auf dem einen Rechner entschlüsselt, im Klartext übertragen und dann auf dem Zielsystem wieder verschlüsselt, somit ist die Datei während der Übertragung nicht geschützt. Hinzukommt, dass die Datei auf dem Zielrechner mit einem anderen Schlüssel verschlüsselt wurde, da der Verschlüsselungsalgorithmus einen zufälligen Schlüssel enthält.

Gegenmaßnahmen

Dieser Sicherheitslücke muss man mit anderen Möglichkeiten, die Windows 2000 bietet, entgegentreten. Es bietet sich IPSec für die Verschlüsselung der Übertragung an, wenn man das IP-Protokoll benutzt.

Verlust der EFS-Schlüssel durch Systemverlust

Gesetzt den Fall, man hat verschlüsselte Daten auf einer zweiten Festplatte oder einem Backupmedium mit einem Windows 2000 konformen Backup-Programm, das die Verschlüsselung aufrecht erhält, gesichert und das Betriebssystem wird unbrauchbar, hat man nach einer Neuinstallation keine Möglichkeit an seine verschlüsselten Daten heranzukommen. Auch wenn man den Benutzer gleich benennt, wird er nicht in der Lage sein, die Datei zu lesen, da die Schlüssel auf dem System nicht mehr vorhanden sind und er eine andere SID, als der damals gleichnamige Benutzer, besitzt. Die verschlüsselten Daten sind somit verloren.

Gegenmaßnahmen

Falls man verschlüsselte Dateien auf seinem Rechner speichert, wurde bereits empfohlen, den privaten Wiederherstellungsagentenschlüssel auszulagern, um die Sicherheit des Systems zu erhöhen. Man kann zur Sicherheit auch noch eine Kopie des privaten Benutzerschlüssels anfertigen. Ist dies geschehen, so ist es problemlos möglich, diesen Schlüssel nach der Neuinstallation wieder zu importieren. Dafür muss man als Administrator oder neuer Wiederherstellungsagent angemeldet sein und die Sicherungsdatei des alten Benutzers, welche an der Dateiendung .fpx zu erkennen ist, mit der rechten Maustaste anklicken und FPX installieren wählen. Damit wird der Zertifikatsimportassistent gestartet und mit diesem das Zertifikat zu den lokal vorhandenen hinzufügen. Danach kann man seine verschlüsselten Daten wieder lesen.

Bei Verschlüsselung auf einer NTFS4-Partition wird Konvertierung vorgemerkt

Falls man noch eine NTFS4-Partition von Windows NT 4.0 in seinem System hat, aus welchen Gründen auch immer, wird diese, bei dem Versuch eine Datei auf einer NTFS4-Partition zu verschlüsseln, sofort für eine Konvertierung in eine NTFS5-Partition vorgemerkt, obwohl man das vielleicht gar nicht möchte.

Gegenmaßnahmen

Es sind keine Gegenmaßnahmen bekannt. Man könnte von vornherein NTFS4-Partitionen in einem Windows 2000 System in NTFS5 konvertieren lassen, andererseits stellt dies auch nicht wirklich eine Sicherheitslücke, sondern nur ein Ärgernis, dar.

Aktualisierte Version von cipher.exe

Microsoft hat eine neue Version von ‚cipher.exe' veröffentlicht, mit der man gelöschte Daten auf der Festplatte des Computers permanent löschen kann. Dadurch werden Daten sicher von der Festplatte entfernt. Ohne diese Erweiterung könnte man mit Tools die Dateien wieder lesbar machen.

4.1.5 Netzwerk

Generell sollte man um sein Netzwerk eine Firewall spannen, die alle außer den unbedingt nötigen Ports blockiert und Zugriffe von außen durch eventuelle Angreifer für eine spätere Analyse protokolliert. Auf diese Weise kann man hinter der Firewall die Netzwerkzugriffe für Mitarbeiter auf vielen Ebenen ermöglichen, ohne dass der Zugriff von außen möglich wird. Es ist jedoch sehr zu empfehlen, die nicht benötigten Ports zusätzlich individuell auf den Rechnern im Netzwerk zu deaktivieren, für den Fall, dass ein Angreifer durch die Firewall hindurchgelangt. Hiermit wird ihm das weitere Vorgehen im Netzwerk wesentlich erschwert, leider vernachlässigen diesen Punkt viele Systemadministratoren, da sie sich durch die Firewall in Sicherheit wiegen. Die folgende Tabelle enthält eine Übersicht der offenen Ports auf einem unveränderten Windows 2000 Domänencontroller:

Port	Dienst
TCP 25	SMTP
TCP 21	FTP
TCP / UDP 53	DNS
TCP 80	WWW
TCP / UDP 88	Kerberos
TCP 135	RPC / DCE Endpoint-Mapper
UDP 137	NetBIOS-Namensdienst
UDP 138	NetBIOS-Datagrammdienst
TCP 139	NetBIOS-Session-Dienst
TCP / UDP 389	LDAP
TCP 443	HTTP über SSL / TLS
TCP / UDP 445	Microsoft SMB / CIFS
TCP / UDP 464	Kerberos kpasswd
UDP 500	Internet Key Exchange, IKE (IPSec)
TCP 593	HTTP RPC Endpoint-Mapper
TCP 636	LDAP über SSL / TLS
TCP 3268	AD Globaler Katalog
TCP 3269	AD Globaler Katalog über SSL
TCP 3289	Windows Terminal Server

Tabelle 4-1 „Eine Auswahl an offenen Ports an einem Windows 2000-Domänencontroller in der Standardkonfiguration" [KUR 01]

Ein allgemeines Problem besteht in der Belassung der Standardkonfiguration und dem Offenlassen von Ports, die nicht benötigt werden. Ein Internet-Host benötigt beispielsweise die Ports 135 bis 139 (NetBIOS), die für Windows-Freigaben zuständig sind, nicht unbedingt und deshalb sollte man sie schließen, indem man in der Netzwerksystemsteuerung von Windows 2000 die Bindung an den WINS-Client entfernt. Das Problem ist damit unter Windows 2000 allerdings noch nicht vollständig gelöst, da es nach wie vor SMB über Port 445 für Windows Dateifreigaben benutzt. Nun können Angreifer zwar nur noch von Systemen mit Windows NT 4.0 Service Pack 6a oder

Windows 2000 aus angreifen, da nur diese Port 445 benutzen können, das ist jedoch ein schwacher Trost und es wird empfohlen, dies durch Entfernen der Bindung zwischen dem Netzwerkadapter und der Datei- und Druckerfreigabe zu lösen. Dies kann man, indem man in den Netzwerkeigenschaften den gewünschten Adapter auswählt und die Einstellung unter Erweitert in Erweiterte Einstellungen vornimmt. Somit kann man sich über NetBIOS nicht mehr auf diesem Rechner anmelden oder Passwortangriffe oder ähnliches durchführen.

Ein wichtiger Schritt um Netzwerke sicher zu machen, ist die Trennung von Ports. Man weist beispielsweise der Protokollierung, der Ansicht der Performancedaten und den Anmeldedaten verschiedene Ports zu, so dass man in der Netzwerkumgebung granulare Zugangsmechanismen durchsetzen kann. Windows NT 4.0 und auch Windows 2000 sind hier furchtbar durchgesetzt. Fast jeder Dienst benutzt SMB über NetBios (Port TCP / 139), bei Windows 2000 ist es etwas besser geworden, Kerberos-Logon benutzt (TCP / 88 und UDP / 88) und LDAP (Port TCP / 389), um auf das Active Directory zugreifen zu können. Dadurch kann man sehr schwer große Netzwerke mit Windows NT 4.0 / 2000-Servern in einem großen Netzwerkverbund sicher machen, da alle die gleiche Kommunikation benutzen und wenn ein Angreifer zu einem der Server Zugang erhält, hat er auch Zugriff zu allen anderen. NetBIOS wurde nicht mit Sicherheitsaspekten konzipiert und es wird davon abgeraten es in zu sichernden Netzwerken einzusetzen, da man sonst mehrere Firewalls und reverse Proxys einsetzen sollte. Die folgende Abbildung zeigt ein Beispielkonfinguration:

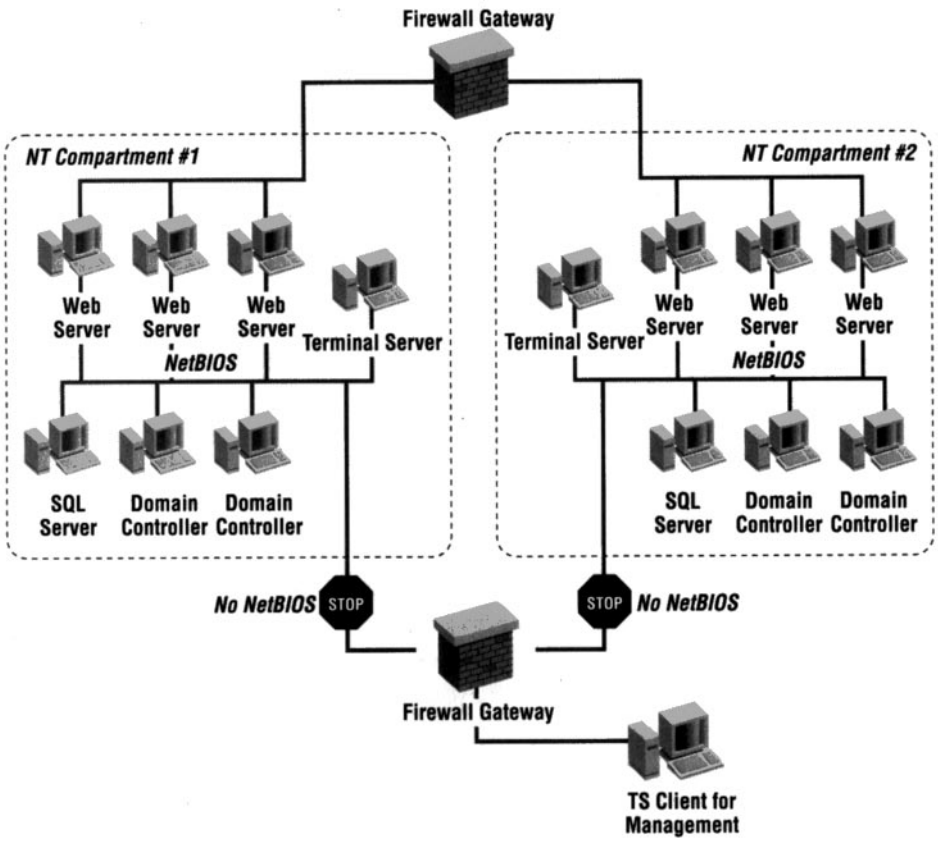

Abbildung 4-3 „NT domains in the perimeter" [NOR01]

In Windows 2000 sind Angriffe durch eine bestimmte Form von ICMP-Paketen möglich. Eine gute Maßnahme besteht in der Verwendung von IPSec, da damit auch keine ICMP-Angriffe mehr möglich sind. Der normale Windows-Paketfilter fängt diese nicht ab, man sollte trotzdem seine Funktionalität nutzen, um andere Arten von Paketen abzufangen. Außerdem kann man IPSec als eine Art Firewall einsetzen, um z.B. nur Port 80 für das World Wide Web durchzulassen und alle anderen zu blockieren. Zusätzlich kann man ping und ICMP verbieten, was dazu führt, dass bei einem externen Portscan nur Port 80 angezeigt wird. Konfigurieren kann man dies mit Hilfe der Anwendung ‚ipsecpol.exe', die im Resource Kit oder auf den Internetseiten von Microsoft erhältlich ist, sowie in den ‚IP-Sicherheitsrichtlinien auf dem lokalen Computer' unter ‚IP-Filterlisten und Filteraktionen verwalten'.

Über DoS-Angriff Kerberos lahm legen und NTLM Authentifizierung erzwingen

Ein Angreifer könnte durch Denial-of-Service-Angriffe auf Kerberos (Port 88) Kerberos lahm legen. Die Windows 2000 Implementation schreibt in diesem Fall vor, dass Windows 2000 auf NTLM zurückgreift und die Authentifizierung hiermit durchführt, bis der Kerberos Dienst wieder verfügbar ist. NTLM Beglaubigungen sind allerdings leicht abzufangen und zu knacken (siehe Kapitel 3.6). Ein SMB-Paket-Abfang-Utility von L0phtcrack beispielsweise kann auch unter Windows 2000 NTLM Beglaubigungen abfangen und knacken. Auf diese Weise ist es ein Leichtes Passwörter abzufangen.

Gegenmaßnahmen

Es gibt keine Gegenmaßnahmen, da das Heruntergehen in der Sicherheit von Kerberos auf NTLM für ein Problem in Kerberos fest in Windows 2000 vorgesehen ist, um den Clients ein Weiterarbeiten zu ermöglichen.

Abgreifbare Kennwort-Hashsequenzen

Kennwort Hashsequenzen von Lan Manager (LM) und NT Lan Manager (NTLM) sind bei der Kommunikation zwischen Windows 2000 und älteren Windows-Rechnern, z.B. Windows NT 4.0, Windows 95 und 98, abgreifbar. Das liegt daran, dass auch wenn Kerberos definiert ist, für Clients die Kerberos nicht beherrschen, also die oben genannten Vorgängerversionen von Windows 2000, auf den alten LM- und NTLM-Hash-Dialog umgeschaltet wird. Diese sind mit Tools abhörbar und somit sind gemischte Netzwerke sehr unsicher, weil sie die gleiche Angriffsfläche bieten wie ein Netzwerk unter Windows NT 4.0.

Gegenmaßnahmen

Die einzige Maßnahme gegen dieses Problem besteht in einer Aufrüstung sämtlicher Rechner in einem Netzwerk auf Betriebssysteme, die Kerberos-Authentifizierung bieten. Man kann nicht verhindern, dass Windows 2000 NTLM statt Kerberos benutzt, wenn der Client Kerberos nicht unterstützt.

Registrierungswerte für SNMP durch SNMP-Pakete änderbar

Da bei Windows 2000 standardmäßig SNMP nicht installiert ist, trifft diese Sicherheitslücke nur auf Rechner zu, auf denen es aktiviert wurde. Die Sicherheitslücke wird im *Microsoft Security Bulletin MS 00-096* beschrieben, durch die unter bestimmten Umständen Registrierungswerte für

SNMP-Parameter, RAS-Parameter und MTS-Paket-Parameter durch speziell geformte SNMP-Nachrichten geändert werden können. Da bei installiertem SNMP Pakete durch das Netzwerk fließen, braucht ein Angreifer diese nur abzufangen und nach seinen Wünschen zu verändern.

Gegenmaßnahmen

Bei Microsoft ist ein Hotfix erhältlich, der dieses Problem behebt. Auf die meisten Rechner wird dieser Bug jedoch nicht zutreffen, da SNMP nur selten benötigt wird.

Schwachstelle im Netzwerkmonitor

Für Servervarianten von Windows 2000 existiert ein optional installierbares Tool namens Netzwerkmonitor (‚netmon.exe'). Es gibt laut *Microsoft Security Bulletin MS 00-083* einen Bug, der bewirkt, dass ein Angreifer, während ein Administrator den Netzwerkmonitor benutzt, um Netzwerkverkehr zu beobachten, ein speziell missgeformtes Paket an den Rechner schicken und damit entweder netmon zum Absturz bringen oder eigenen Code im Sicherheitskontext des Administrators ausführen kann. Somit könnte der Angreifer Kontrolle über den Rechner bekommen, da er administrative Rechte ausnutzen kann.

Gegenmaßnahmen

Es gibt einen Hotfix von Microsoft, der nicht in Service Pack1, aber in Service Pack 2 enthalten ist und dieses Problem im Netzwerkmonitor behebt.

Gespoofte NetBIOS Name Server

Ein Fehler, der in *Microsoft Security Bulletin MS 00-047* beschrieben wird, ermöglicht das Spoofen von NetBIOS Name Server Protokollen. Wird dies erfolgreich durchgeführt, scheint es für anfragende Clients so, als wäre der Server nicht mehr vorhanden oder erreichbar und sie können sich nicht mehr anmelden; der Fehler ermöglicht insofern einen Denial-of-Service-Angriff. Wenn Port 137 (UDP) deaktiviert ist, ist dieser Angriff vom Netzwerk aus nicht möglich.

Gegenmaßnahmen

Auf den Microsoft-Internetseiten kann ein Hotfix heruntergeladen werden, durch welchen es möglich wird, sichere Einstellungen für NetBIOS Name Server vorzunehmen; ein geringes Restrisiko bleibt jedoch, da diese Einstellungsmöglichkeiten wahrscheinlich nicht alle Probleme abdecken.

Fehlerhafte Reassemblierung von IP-Paketen

Ein Fehler bei der Reassemblierung von IP-Paketen, der in der gesamten Windows-Familie vorhanden ist, führt zur totalen Auslastung der CPU, wenn ein Angreifer ein speziell missgeformtes IP-Datagramm kontinuierlich an ein Ziel sendet. Der Zielrechner ist dann mit dem Bearbeiten und Reassemblieren der Pakete komplett ausgelastet. Der Angreifer kann das System damit bis zum Absturz bringen, sich aber keine Rechte erobern oder Zugriff auf Daten erlangen.

Gegenmaßnahmen

Für dieses Problem hat Microsoft auf den Internetseiten für jedes Betriebssystem jeweils einen Patch bereit gestellt, der das Problem behebt.

Keine Protokollierung fehlerhafter Anmeldeversuche über IP

In Windows 2000 werden fehlgeschlagene Anmeldeversuche über IP immer noch nicht protokolliert. Diese Sicherheitslücke gibt es beispielsweise in UNIX-Systemen nicht und es ist nicht verständlich, warum es in Windows 2000 nicht integriert wurde.

Gegenmaßnahmen

Gegen diese Sicherheitslücke existieren leider keine Maßnahmen, da es keine Möglichkeit zur Protokollierung fehlerhafter Anmeldeversuche über IP gibt.

Sperrung von Port 500 und 88 auf Domänencontrollern nicht möglich

Auf Domänencontrollern lassen sich Port 500 (UDP) oder 88 (TCP / UDP) nicht sperren, da sie für die IPSec-Authentifizierung mit Kerberos (Port 88) oder IKE (Port 500) erforderlich sind. Daraus ergibt sich eine Sicherheitslücke.

Gegenmaßnahmen

Nach der Installation von Service Pack 1 für Windows 2000 kann man in der Registrierung den Kerberos-Port durch die Deaktivierung einer Ausnahmeregel in HKLM\CurrentControlSet\Services\IPSEC\NoDefaultExempt sperren.

4.1.6 Kerberos v5

Kerberosverkehr ist trotz IPSec unverschlüsselt

Microsoft hat am 18.11.2000 ein Dokument auf dem Microsoft Webserver veröffentlicht [URL07], in dem bekannt gegeben wird, dass Kerberos-Datenverkehr zwischen Domänencontrollern, bei denen der Datenverkehr durch IPSec geschützt sein soll, nicht verschlüsselt wird. Der Grund hierfür ist in der IPSec Implementation zu suchen, die einige Datentypen von der Verschlüsselung ausklammert, nämlich Broadcast, Multicast, RVSP, IKE und Kerberos.

Gegenmaßnahmen

Es gibt einen Hotfix für dieses Problem und der Patch ist in Service Pack 1 enthalten und sollte auf allen Domänencontrollern installiert sein. Zusätzlich zur Installation des Patches muss man einen Wert in der Registrierung hinzufügen: in HKLM\SYSTEM\CurrentControlSet\Services\IPSEC muss der Wert „NoDefaultExempt“ vom Typ „REG_DWORD“ mit Wert auf „1“ gesetzt werden. Ist dieser Wert auf „0“ gesetzt, werden die oben genannten Datentypen weiterhin nicht verschlüsselt.

Zu hohe Lebensdauer von TGTs

Eine zu hohe Lebensdauer von Ticket Granting Tickets könnte ein Sicherheitsproblem darstellen, da sie von Angreifern, die Zugriff zu einem angemeldeten Rechner erlangen, genutzt werden können, um eine andere Identität vorzutäuschen.

Gegenmaßnahmen

Die Konfiguration von TGTs mit geringerer Lebensdauer erhöht die Sicherheit, führt jedoch zu häufigerer Anforderung und Ausstellung von TGTs, was den Netzwerkverkehr erhöht.

Unsichere Konfiguration aus Performancegründen

Genau wie bei IPSec könnten die Administratoren weniger sichere Einstellungen wählen, um den Netzwerkverkehr zu reduzieren.

Gegenmaßnahmen

Es sollte eine Überprüfung stattfinden, ob ein erreichter Performancegewinn die Verringerung der Sicherheit wert ist.

Auf weitergehende Kerberosspezifische Probleme gehen wir in dieser Arbeit nicht ein.

4.1.7 Infrastruktur öffentlicher Schlüssel (PKI)

Schlüssel sind auf der Festplatte des Rechners gespeichert

Die Schlüssel werden normalerweise auf der Festplatte des Rechners gespeichert, falls der Rechner nicht in einer Domäne steht. Im zweiten Fall werden die Schlüssel nur auf dem Domänencontroller gehalten und bei einer erfolgreichen Anmeldung an diesem stehen sie zur Verfügung.

Gegenmaßnahmen

Es gibt für Benutzer, die nur über einen Einzelplatzrechner oder ein Netzwerk ohne Domänencontroller verfügen, keine Möglichkeit die Schlüssel für die PKI auszulagern. Im Falle, dass jemand den eigenen privaten Schlüssel benutzt, muss man dies unverzüglich der Zertifizierungsstelle mitteilen und diese trägt das eigene Zertifikat in die Zertifikatsrückziehungsliste (Certificate Revocation List) ein.

Verlust des privaten Schlüssels

Der Verlust des privaten Schlüssels für die PKI ist verheerend, im Besonderen der einer Zertifizierungsstelle, da das Vertrauen dieser dann untergraben ist. Dieser Zertifizierungsstelle würde niemand mehr trauen und man müsste eine neue Zertifizierungsstelle aufsetzen und alle Zertifikate erneuern. Im Falle des Verlusts eines privaten Schlüssels eines Benutzers, kann dieser nicht einmal seinen öffentlichen Schlüssel zurückziehen oder in einer Zertifikatsrückziehungsliste eintragen lassen, da er sich nicht authentifizieren kann und andere werden immer noch versuchen über diesen Schlüssel mit ihm zu kommunizieren, wie bei einer bekannten Person geschehen. Es bleibt dem Benutzer nichts anderes übrig, als eine neue Identität anzunehmen und für diese ein neues Schlüsselpaar anzufordern und seinen Kommunikationspartnern mitzuteilen, dass sie den alten Schlüssel nicht benutzen sollen, obwohl er für den eigenen Namen angeboten wird, deshalb kann man sich auch nicht unter diesem Namen ein neues Schlüsselpaar holen, sondern muss einen anderen Namen, als eventuell seinen eigenen, annehmen.

In einem Betrieb ist es natürlich möglich, da man bekannt ist, den Administrator dazu zu bewegen, ein neues Schlüsselpaar auszustellen und somit seinen Namen für das Zertifikat zu behalten.

Gegenmaßnahmen

Es existieren keine Gegenmaßnahmen gegen Schlüsselverlust, weil das die Sicherheit des System der Infrastruktur öffentlicher Schlüssel untergraben würde.

Einige Programme überprüfen die Zertifikatsrückziehungslisten nicht

Ein weiteres Problem zahlreicher Software ist, dass sie, bei einmaliger erfolgreicher Überprüfung, das Zertifikat des Benutzers oder der Gegenstelle speichert und fortan davon ausgeht, dass es gültig ist. Der Internet Explorer beispielsweise überprüft erst seit Version 5.5, ob die gespeicherten Zertifikate in Zertifikatsrückziehungslisten stehen, um sie in dem Fall zu löschen.

Gegenmaßnahmen

Als Gegenmaßnahme eignet sich nur der Einsatz von Software, die regelmäßig Certificate Revocation Lists überprüft.

Wir gehen in dieser Arbeit nicht näher auf allgemeine Probleme von Infrastrukturen öffentlicher Schlüssel ein.

4.1.8 IPSec

Sicherheitslücken durch schlechte Konfiguration

Durch die sehr großen Konfigurationsmöglichkeiten von IPSec, ergibt sich die Möglichkeit von Einstellungen, die Sicherheitslücken offen lassen. Die richtige Konfiguration von IPSec erfordert fundiertes Fachwissen und das Kennen des Konfigurationstools für IPSec in Windows 2000, die Verwendung kann aber zu einer erheblichen Sicherheitssteigerung führen.

Gegenmaßnahmen

Es empfiehlt sich die Konfiguration durch eine Person, die sich in diesem Bereich weitergebildet hat, da einerseits die Möglichkeit einer „Überkonfiguration" besteht, die zuviel Performance fordert, obwohl sie gar nicht angebracht ist, oder einer „Unterkonfiguration", bei der die notwendige Sicherung der Kommunikation nicht gewährleistet wird.

Unsicherheit von AH im alleinigen Einsatz

Mit dem Authentication Header stellt IPSec Authentifizierung, Anti-replay und Integrität für das gesamte Paket sicher. Eine Verschlüsselung des Paketes findet nicht statt und deswegen kann das Abfangen und Lesen der Pakete nicht verhindert werden. Allerdings können Sender, Empfänger und die Unversehrtheit der Daten gewährleistet werden. AH wird als AH-Header hinter den IP-Header gestellt, somit sind die Pakete für andere, die das Netzwerk abhören, lesbar.

Gegenmaßnahmen

Wenn man sicherheitsrelevante Daten über ein Netzwerk transportiert, sollte man Encapsulating Security Payload in IPSec verwenden. Falls man auch noch sicher stellen muss, dass Integrität und Authentizität des Kommunikationspartners stimmen, muss man ESP mit AH kombinieren.

Unsicherheit von ESP im alleinigen Einsatz

Durch Encapsulating Security Payload bietet IPSec Verschlüsselung, Authentifizierung, Anti-replay und Integrität für das gesamte Paket. Mit ESP werden die Daten in der eigenen Protokollstruktur gekapselt, dies ist bei AH nicht der Fall. Der IP-Header wird jedoch nicht signiert, was bei AH geschieht, und deshalb kann ein Angreifer den IP-Header verändern und der Empfänger bemerkt dies nicht einmal.

Gegenmaßnahmen

Falls die Integrität des IP-Headers von entscheidender Bedeutung ist, kann man für diesen Zweck AH mit ESP kombinieren.

Unsichere Konfiguration aus Performancegründen

IPSec kann zu einer starken Belastung des Netzwerks durch IKE-Verkehr und Header führen und die Prozessorauslastung durch Ver- und Entschlüsselungs-Vorgänge und Integritätsberechnung erhöhen. Ist die maximale Sicherheit durch alle Optionen gewählt, kann es zu deutlichen Performanceverlusten kommen. Aus diesem Grunde werden viele Systemadministratoren sicherlich eine unsicherere Konfiguration vorziehen, da sie den Performanceverlust in einem, nach ihrem Ermessen, erträglichen Rahmen hält.

Gegenmaßnahmen

Es sollte klar festgelegt werden, welche Sicherheitsmaßnahmen benötigt werden und diese sollten dann auch in der Konfiguration komplett umgesetzt werden. Es ist keinem damit geholfen, wenn Verschlüsselung und Transport schneller sind, dafür aber die Daten nicht sicher genug geschützt werden.

ESP-Tunnel nur für IP-Netzwerke nutzbar

Man kann ESP-Tunnel leider nur für IP-Netzwerke benutzen, da dieser Tunnel auf der OSI-Schicht 3 arbeitet und keine außer den IP-Paketen tunneln kann. Somit ist diese Einstellung von IPSec in gemischten Windows-Netzwerken nicht nutzbar, da nicht alle Clients sie verwenden können.

Gegenmaßnahmen

Es bietet sich nur die Nutzung von homogenen Windows-Netzwerken oder solchen, die ausschließlich IP benutzen, an, wenn man die Sicherheit von ESP in IPSec benötigt.

4.1.9 Secure Sockets Layer (SSL) und Transport Layer Security (TLS)

SSL und TLS werden im Internet hauptsächlich für die sichere Übertragung und Authentifizierung von Web-, Mail- oder Newsserver verwendet. Durch die Vergabe von Zertifikaten an Firmen durch Zertifizierungsstellen kann ein Benutzer einem Dienst, der von dieser Firma angeboten wird und für den das Zertifikat erstellt wurde, insofern vertrauen, als dass dieser wirklich von der Firma angeboten wird und die Daten verschlüsselt werden. Ob die Firma oder der Dienst vertrauenswürdig ist oder vertrauenswürdig mit Daten umgeht, wird natürlich nicht sichergestellt, die Zertifizierungsstelle kann nach Ausgabe des Zertifikats diese Firma nicht ständig kontrollieren.
In Windows 2000 Netzwerken können eigene Zertifizierungsstellen eingerichtet werden, die dann innerhalb des Unternehmens vertrauenswürdig sind und eigene Zertifikate ausstellen können. Diese können für Serverdienste (z.B. interne Webdienste) oder für Benutzer verwendet werden, die sich dann mit diesem Zertifikat authentifizieren können.

Nicht vertrauenswürdige Zertifikate

Die Vergabe von Zertifikaten ist eine komplizierte Angelegenheit. Wie soll eine Zertifizierungsstelle in den USA, ein Zertifikat für eine Website einer Firma, die ihren Sitz irgendwo in Süddeutschland hat, ausstellen und die Echtheit der Zertifikatsanforderung genau überprüfen können? Wird jede Anforderung wirklich hundertprozentig überprüft und wirklich festgestellt, ob nicht das Konkurrenzunternehmen dieses Zertifikat angefordert hat? Es ist natürlich jedem Internetuser selbst überlassen, ob er einer Zertifizierungsstelle und den ausgestellten Zertifikaten vertraut, aber das Misstrauen wird ihm auch nicht weiterhelfen und viele Zertifikate von Zertifizierungsstellen sind in heutigen Browsern bereits integriert und werden selten von einem Benutzer überprüft.
Innerhalb eines Unternehmens ist dies nicht anders. Hat ein Unternehmen eine gewisse Größe erreicht oder ist es z.B. über mehrere Länder verteilt, kann auch hier eine Kontrolle schwierig werden.

Gefahren

Vertraut ein Benutzer einem Zertifikat und ist dieses Zertifikat falsch, liegt es im Ermessen desjenigen, der das Zertifikat verwendet, welchen Schaden er anrichten möchte. Im Web könnte es sich um private Daten eines Benutzer handeln, die der Angreifer erfahren möchte. Auch das Ausführen von signierten Scripten in einem Webbrowser ist eine Gefahr, wenn durch solche Scripte Daten manipuliert oder unberechtigt gelesen werden können. Windows 2000 verwendet Zertifikate für viele Zwecke. Softwareupdates werden von Microsoft signiert und Software- bzw. Hardwarehersteller können Dateien von Microsoft signieren lassen.
Die Verwendung von Software oder Treiber, die mit einem falschen Zertifikat signiert worden sind, kann Risiken beinhalten und Trojaner oder Backdoors in einem System einschleusen.

Bekannte Sicherheitsprobleme

Fehlerhafte Ausgabe von Zertifikaten durch VeriSign Inc.

Microsoft hat in Artikel MS01-017 im Microsoft Security Bulletin bekannt gegeben, dass VeriSign Inc. zwei Zertifikate zur Code-Signierung ausgegeben hat, die den Firmennamen „Microsoft Corporation" enthalten und an jemand ausgegeben wurden, der nicht zum Unternehmen Microsoft gehört.

„In mid-March 2001, VeriSign, Inc., advised Microsoft that on January 29 and 30, 2001, it issued two VeriSign Class 3 code-signing digital certificates to an individual who fraudulently claimed to be a Microsoft employee. The common name assigned to both certificates is "Microsoft Corporation"." [MS01-017]

Diese Zertifikate können dazu verwendet werden, Programme, ActiveX Objekte oder Macros zu signieren. Führt ein Benutzer solch ein Programm aus, wird eine Meldung erscheinen, dass das Programm von der „Microsoft Corporation" signiert wurde. Dies würde sicherlich dazu führen, dass der Benutzer dem Programm vertraut und es ausführt.

Da das Problem erkannt wurde, hat VeriSign Inc. das Zertifikat zurückgenommen und es erscheint in der *Certificate Revocation List (CRL)*, die alle zurückgezogenen Zertifikate auflistet. Leider enthält das Zertifikat keine Internetadresse der CRL, so dass ein Installationsprogramm oder Internetbrowser nicht in der Lage ist, diese Liste zu überprüfen.

„VeriSign has revoked the certificates, and they are listed in VeriSign's current Certificate Revocation List (CRL). However, because VeriSign's code-signing certificates do not specify a CRL Distribution Point (CDP), it is not possible for any browser's CRL-checking mechanism to locate and use the VeriSign CRL." [MS01-017]

Microsoft hat ein Update veröffentlicht, das diese Zertifikate erkennt und den Benutzer warnt, wenn sie verwendet werden. Weitere Informationen hat Microsoft in der Microsoft Knowledge Base, Artikel Q293819 veröffentlicht. Der Patch wurde in Service Pack 2 für Windows 2000 integriert.

Gegenmaßnahmen

Generell sollte man nicht jeder Software oder jeder Website Vertrauen schenken, nur weil sie signiert wurde oder der Webserver ein Zertifikat besitzt. Zertifikate sind kein hundertprozentiger Schutz und können ebenso missbraucht werden. Die Verwendung von SSL oder TLS als Verschlüsselung im Internet ist immer noch die beste Methode, um Daten sicher zu übertragen.

Verlust des privaten Schlüssels

SSL bzw. TLS verwenden für die Authentifizierung und Verschlüsselung ein kryptografisches Verfahren, das auf einem asymmetrischen Schlüsselpaar des Webservers basiert. Während der öffentliche Schlüssel von einer Zertifizierungsstelle signiert wurde und jeder Client das erstellte Zertifikat und den öffentlichen Schlüssel erhalten darf, muss der private Schlüssel gut geschützt werden. Wird er entwendet, dann ist die Sicherheit der Übertragung gefährdet und jede Verwendung des Schlüsselpaares wird nutzlos.

Gefahren

Wird ein privater Schlüssel von einem Webserver entwendet, kann sich evtl. ein anderer Server als der ursprüngliche Webserver ausgeben. Auch das Entschlüsseln der Daten wird dann unter gewissen Umständen möglich, da der Sitzungsschlüssel erstellt werden kann. Es ist also sowohl die Verschlüsselung als auch die Authentifizierung nicht mehr gewährleistet.

Bekannte Sicherheitsprobleme

„Windows 2000 verwaltet das Paar aus privatem und öffentlichem und das Zertifikat des IIS-Servers. Sie sollten daran denken, dass der private Schlüssel normalerweise ungeschützt in der Registrierdatei abgelegt wird." [ISS00]
Die einfache Speicherung des privaten Schlüssels in der Registrierung ist sicherlich kein ausreichender Schutz und muss durch eine gute Sicherung des Servers ergänzt werden.

Gegenmaßnahmen

Da das Entwenden des privaten Schlüssels katastrophale Folgen für eine Website haben kann, ist es besonders wichtig, diesen Schlüssel zu schützen. Auch wenn Zertifikate zurückgezogen werden können und dann in die CRL der Zertifizierungsstelle eingetragen werden, müssen Clients diese CRL aktiv überprüfen. Natürlich muss der Schlüssel auf dem Server bleiben, da dieser sonst keine Daten verschlüsseln kann, der Server sollte aber nicht nur mit leicht erratbaren Passwörtern geschützt werden, sondern durch eine Firewall ergänzt und sichere Passwörter bekommen.

Überprüfung von zurückgezogenen Zertifikaten

Wird ein Zertifikat von der Zertifizierungsstelle zurückgezogen, wird es in die Certificate Revocation List (CRL) der Zertifizierungsstelle eingetragen. Die URL dieser CRL ist normalerweise Bestandteil des Zertifikat und ein Client kann damit ein Zertifikat auf Gültigkeit überprüfen. Diese Funktion muss natürlich aktiviert sein, damit eine Überprüfung stattfindet und eine es muss eine URL im Zertifikat eingetragen sein.

Gefahren

Wird ein Zertifikat zurückgezogen, hat das sicherlich gute Gründe. Wie bereits erwähnt, kann das Abhandenkommen von privaten Schlüsseln oder das nachträgliche Erkennen von Fehlern während der Zertifizierung dazu führen.

Bekannte Probleme

Die Überprüfung eines Zertifikats wird durch den Client vorgenommen, der das Zertifikat von einem Server erhalten hat (bei Clientzertifikaten ist es andersherum). Die Internetoptionen erlauben das Aktivieren und Deaktivieren der Überprüfung von Serverzertifikaten. Werden die Einstellungen auf die Standardwerte zurückgesetzt, sind beide Überprüfungen deaktiviert und müssen manuell wieder aktiviert werden.

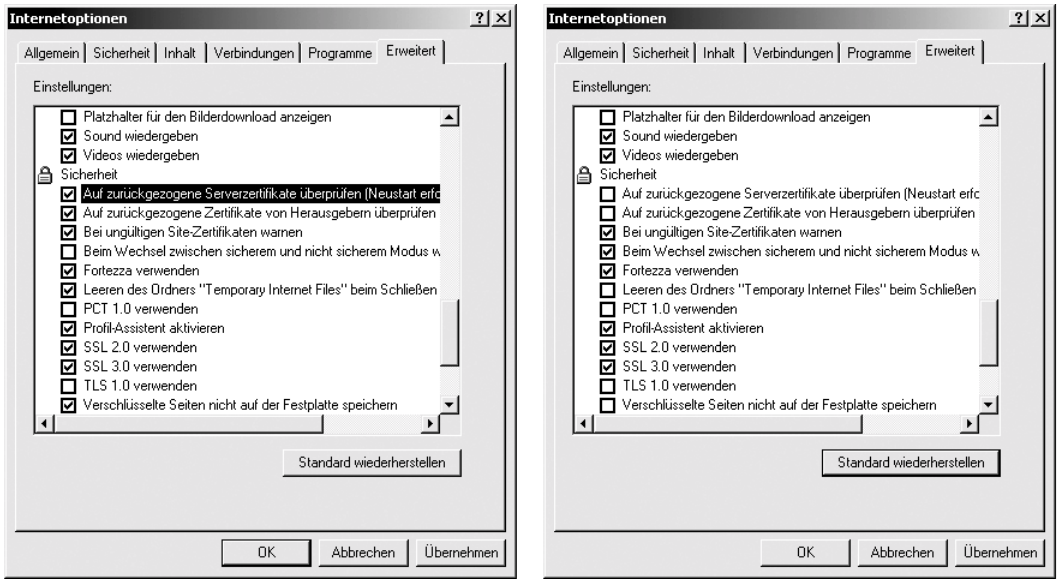

Abbildung 4-4 Auswählen der Standardeinstellungen deaktiviert die Zertifikatsüberprüfung

Außerdem enthält nicht jedes Zertifikat eine URL für die CRL. Da dies kein Problem von Windows 2000 ist, wurde dem aber weiter nachgegangen. Es hat aber erhebliche Schwierigkeiten bei der Suche nach einer CRL einer bekannten Zertifizierungsstelle gegeben und die Überprüfung einiger Testzertifikate auf aktuelle Gültigkeit wurde nach erfolglosen Versuchen von uns schließlich abgebrochen.

Gegenmaßnahmen

Das Zurückziehen von Zertifikaten hat nur Sinn, wenn dies auch überprüft wird bzw. werden kann. Daher sollten die Überprüfungen unbedingt aktiviert werden. Das gilt für jede Software, die Zertifikate verwendet. Natürlich muss das Programm auch die Möglichkeit haben, eine Verbindung zur Website der Zertifizierungsstelle herzustellen und eine Firewall muss diese Verbindung ggf. erlauben.

4.2 Integrierte Komponenten

Windows 2000 beinhaltet viele integrierte Dienste und Komponenten, die vom Betriebssystem oder von Anwendungen verwendet werden. Dienste, wie der DNS-Server oder der IIS-Dienst, erweitern die Einsatzgebiete von Windows 2000, allerdings ist die Installation bzw. Nutzung solcher Dienste mit Risiken verbunden und die Konfiguration dieser Komponenten trägt einen wesentlichen Beitrag zur Sicherheit des gesamten Systems bei.
Dieses Kapitel beschreibt wichtige Einstellungen, die das System sicherer gegen Angriffe machen und zeigt einige häufig gemachte Fehler bei der Konfiguration. Außerdem werden bekannte Sicherheitsprobleme und deren Lösung besprochen.

4.2.1 Component Object Model (COM,DCOM) und COM+

COM verwendet Remote Procedure Calls als Transportmechanismus über das Netzwerk. Der Aufruf von COM-Objekten über das Netzwerk ist ein Vorgang, der für verteilte Anwendungen und Server/Client basierte Systeme verwendet wird. Durch die Verwendung von RPCs für den Aufruf von COM-Objekten über das Netzwerk, ist die Sicherheit von RPC mit entscheidend.
RPCs verwenden dabei unterschiedliche Transportprotokolle, die evtl. über eigene Sicherheitsmechanismen verfügen. So können z.B. Named Pipes verwendet werden, die allerdings nur unter Windows NT bzw. Windows 2000 funktionieren.
Die Authentifizierung findet durch den *Security Support Provider (SSPI)* statt. Dieser kann verschiedene Sicherheitsprotokolle verwenden:

- **LanManager Authentifizierung (NTLMSSP)**
  Diese Authentifizierung ist auch in Windows 9x und älteren NT-Versionen enthalten und erlaubt die Verwendung der Authentifizierung mit diesen Systemen.
- **Kerberos v5**
  Kerberos ist das Standardprotokoll in Windows 2000.
- **Schannel**
  Diese Authentifizierung verwendet SSL und die *Private Communications Technology (PCT)*
- **Snego**
  Dieses Sicherheitsprotokoll verwendet automatisch das beste zur Verfügung stehende Protokoll.

Sicherheitseinstellungen für COM Objekte

COM verwendet zwei verschiedene Sicherheitskategorien. Die programmatische Sicherheit wird durch die Komponente selbst vom Entwickler zur Verfügung gestellt, sie prüft, ob ein Aufruf gestattet oder verweigert wird.

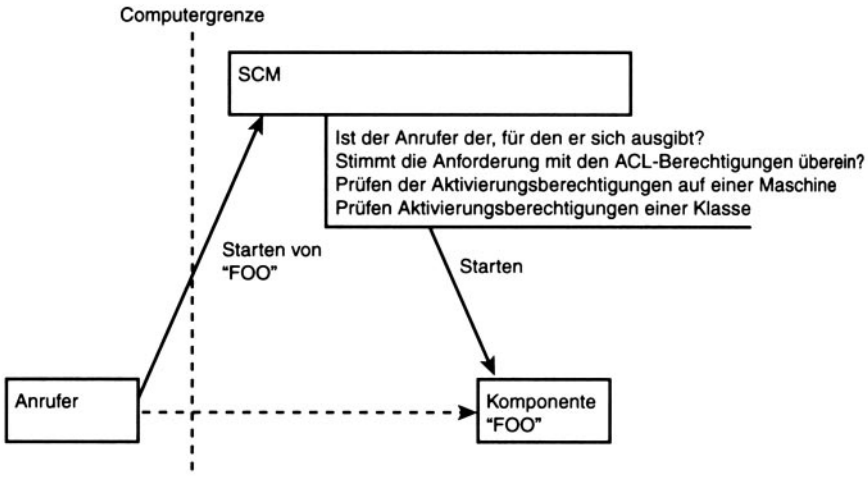

Abbildung 4-5 „Sicherheitsprüfung durch das System beim Aufrufen einer Instanz einer Server-Komponente" [SCH01]

Die deklarative Sicherheit wird außerhalb der Komponente festgelegt und mit Programmen wie ‚RegEdit', ‚RegEdt32' oder ‚DCOMCnfg' eingerichtet. Dabei können einzelne Komponenten mit unterschiedlichen Sicherheitseinstellungen konfiguriert werden, die verwendeten Netzwerkverbindungen werden festgelegt und die Komponenten können über DACLs geschützt werden. Der *Service Control Manager (SCM)* überprüft bei einem Aufruf die Identität des Clients und stellt fest, ob dieser berechtigt ist, den Aufruf durchzuführen. Ist er nicht berechtigt, wird der Aufruf verweigert.
Sinnvoll kann auch eine Mischung von beiden Sicherheitsmaßnahmen sein, wenn z.B. eine Gruppe von Benutzern Zugriff auf eine Komponente bekommen soll, einige Benutzer eine einzelne Funktion der Komponente aber nicht aufrufen dürfen. Dann werden beide Sicherheitskategorien verwendet und die Komponente entscheidet, welche Funktionen von welchem Benutzer aufgerufen werden dürfen.

COM+

COM+ verbindet nun die COM-Komponenten mit dem Microsoft Transaction Server (MTS). Dabei kann eine COM+-Komponente die Sicherheitsfunktionen von COM Objekten weiterhin benutzen, es sind aber *rollenbasierte Sicherheitseinstellungen* hinzugekommen.

Deklarative Sicherheit

COM+-Anwendungen sind Zusammenstellungen von COM und COM+-Komponenten zu einer Anwendung. Diese wurden früher als Pakete bezeichnet. Die deklarative Sicherheit für eine COM+-Anwendung wird mit dem Verwaltungsprogramm für Komponentendienste eingerichtet. Dort werden auch die rollenbasierten, deklarativen Sicherheitseinstellungen vorgenommen.

Prozedurale Sicherheit

Ist die deklarative Sicherheit nicht ausreichend, können Entwickler weitere Sicherheitsprüfungen in den Programmcode der Komponente einbauen. COM+ bietet einem Entwickler weitere Funktionen, mit denen er z.B. feststellen kann, ob prozedurale Sicherheit für eine Komponente aktiviert ist und ob der Client eine bestimmte Rolle hat.

Verwaltung der COM+-Sicherheit

Windows 2000 bietet eine Reihe von Anwendungen, mit denen ein Administrator die deklarativen Sicherheitseinstellungen für COM+-Komponenten vornehmen kann.

- **DCOMCnfg**
  Dieses Tool ermöglicht die Festlegung der Berechtigungen für DCOM- und COM-Komponenten und kann auch zur Konfiguration der verwendeten Netzwerkprotokolle eingesetzt werden.
- **Verwaltungsprogramm für Komponentendienste**
  Dieses Programm benutzt die Microsoft Management Konsole (MMC) und erleichtert die Einrichtung der deklarativen Sicherheit für COM+-Anwendungen.

DoS Angriff durch RPC-Aufrufe

Wie im Dokument MS01-041 beschrieben wird, können fehlerhafte RPC-Aufrufe zu DoS-Angriffen führen. Betroffen sind viele Systemdienste die RPCs verwenden. Dazu gehören der Exchange Server 2000, der SQL Server 7.0, der SQL Server 2000 und weitere Systemdienste von Windows 2000.
Laut Microsoft kann ein Angreifer den Fehler nur für DoS-Angriffe ausnutzen und keine Software auf dem System installieren oder sich weitere Zugriffsrechte verschaffen.

Gegenmaßnahmen

Es ist ein Softwareupdate von Microsoft für dieses Problem veröffentlicht worden. Ein weiterer Schutz besteht in der Abschirmung eines Computers durch eine Firewall, die RPC-Aufrufe verhindert.

4.2.2 Dynamic Host Configuration Protocol (DHCP)

Der DHCP-Dienst ist für die Zuteilung von IP-Informationen in einem Netzwerk zuständig. Die automatische Vergabe von IP-Adressen an Clients könnte diese mit falschen Informationen versorgen und ihnen die Möglichkeit nehmen, im Netzwerk zu kommunizieren.

Rouge-Server

Ein nicht autorisierter DHCP-Server wird auch als *Rouge-Server* bezeichnet. Ein Windows 2000 DHCP-Server prüft in einer Windows 2000 Domänen-Umgebung immer, ob er für den Einsatz autorisiert wurde. Ist dies nicht der Fall, wird er die eigene Initialisierung abbrechen. Autorisiert wird ein DHCP-Server durch einen Eintrag im Active Directory, der von dem Server geprüft wird. Damit ist das Netzwerk natürlich nicht vor feindlichen DHCP-Servern geschützt, da diese sich nicht einfach abschalten werden oder eine Autorisierung erst gar nicht prüfen. Clients, die falsche IP-Informationen von einem nicht autorisierten DHCP-Server bekommen, werden entweder nicht in der Lage sein, im Netzwerk zu kommunizieren, oder beispielsweise durch falsche Gateway-Adressen ihre Daten an einen feindlichen Server im Netzwerk schicken, der diese dann auswerten kann. Dabei handelt es sich allerdings nicht um ein spezielles Windows 2000-Problem und betrifft überwiegend gemischte Netzwerke.

Gegenmaßnahmen

Ein Angreifer muss schon einiges erreicht haben, um einen Rouge-Server in einem Netzwerk installieren zu können und mit ihm falsche IP-Daten zu verteilen. Um einen möglichen Schaden einzugrenzen, sollten Server immer manuell konfigurierte IP-Adressen und -Daten verwenden. Windows 2000 Clients können außerdem mit Protokollen wie IPSec gesichert werden, da der Windows 2000 DHCP-Server das IPSec-Sicherheitsmodell unterstützt.

DoS-Agriffe auf DHCP-Server

Wird ein DHCP-Server durch einen Angriff ausgeschaltet, können DHCP-Clients nicht mehr mit IP-Konfigurationen versorgt werden und sind dann nicht mehr in der Lage, im Netzwerk zu kommunizieren. Clients können sich dann nicht mehr anmelden und andere Netzwerkdienste nutzen.

Gegenmaßnahmen

DoS-Angriffe können durch Überlastung eines Dienstes oder durch Programmierfehler in der verwendeten Software entstehen. Das Problem der Überlastung eines Dienstes kann nur durch eine Abschirmung des Servers von gefährdeten Netzwerken behoben werden.
Werden DoS-Angriffe durch Softwarefehler ermöglicht, bleibt nur die Installation eines Softwareupdates.

Bekannte Sicherheitsprobleme

Obwohl der DHCP-Server nicht von direkten DoS-Attacken betroffen ist, bzw. noch keine Angriffe bekannt wurden, kann der TCP/IP-Dienst durch fehlerhafte Anfragen an den "Druckdienst für UNIX", wenn dieser installiert ist, zum Absturz gebracht werden. Von diesem Absturz ist auch der DHCP-Server betroffen.
Dieses Problem wird in dem Microsoft Artikel MS00-021 beschrieben: „TCP/IP Printing Services is an RFC 1179-compliant printing service designed for environments that use the Berkeley Remote Printing protocols, also known as LPD and LPR. (In Windows 2000, TCP/IP Printing Services are also known as Print Services for Unix). A specially-malformed print request could cause TCPSVC.EXE to crash, which would not only prevent the server from providing printing services, but also would stop several other services, most importantly DHCP. Any affected services could be put back into service by restarting them; it would not be necessary to reboot the machine.“ [MS00-021]
Ein Softwareupdate für diesen Fehler ist vorhanden und kann von Microsoft bezogen werden.

4.2.3 NetBIOS-Namensdienst und Windows Internet Name Service (WINS)

Der Windows Internet Name Service wurde schon in NT 4.0 eingesetzt und kann in einem Windows 2000 durch den Verzeichnis- und den DNS-Dienst ersetzt werden. Handelt es sich allerdings um ein gemischtes Netzwerk, wird der WINS-Dienst evtl. noch benötigt.

Kopieren der WINS-Datenbank

Ein Angreifer kann die Informationen, die der WINS-Dienst verwaltet, zur Analyse des Netzwerks und der enthaltenen Computer verwenden. Dieses Vorgehen entspricht einen unerlaubtem Zonentransfer bei einem DNS-Server. Dafür muss der Angreifer allerdings direkten Zugriff zum Server oder zum Systemlaufwerk erhalten.

Gegenmaßnahmen

Der direkte Zugriff zu einem Server sollte abgesichert sein, und ein Administrator sollte sich bei Verlassen des Server abmelden, damit niemand die Sitzung weiter verwenden kann.
Auch die Freigabe des Systemlaufwerks sollte auf einem Server die Ausnahme sein.

DoS-Angriff auf den WINS-Server

Ein Windows 2000 Server kann ohne die nötigen Softwareupdates durch einen DoS-Angriff blockiert werden. Unter Umständen kann dadurch auch der WINS-Server ausfallen und es ergeben sich ähnliche Probleme, wie bei einem DNS-Server-Ausfall, die im Kapitel 4.2.4 beschrieben werden.

Können die Clients den WINS-Server nicht mehr verwenden, werden diese allerdings die NetBIOS-Broadcast-Methoden zur Namensregistrierung und -auflösung verwenden, wenn sie nicht für die alleinige Verwendung des WINS-Dienstes konfiguriert wurden.
Daher wird ein WINS-Server Ausfall nicht unbedingt dazu führen, dass sich Clients nicht mehr im Netzwerk anmelden können, es sei denn, der WINS-Server ist der einzige Domänencontroller.

Gegenmaßnahmen

Gegen DoS-Angriffe hilft nur die Installation von entsprechenden Softwareupdates. Werden diese installiert, sollte ein System gegen bekannte DoS-Angriffe gesichert sein.

Absichtliches Herbeiführen von Namenskonflikten

Ein Netzwerk, das NetBIOS-Namen verwendet, basiert auf das selbstständige Registrieren und Verteidigen von NetBIOS-Namen. Ein Angreifer kann sich diesen Mechanismus zu Nutze machen und die Namensregistrierung anderer Systeme verhindern, indem er diese Namen selbst verteidigt. Dieses Problem wird auch im Microsoft Dokument MS00-047 beschrieben: „The NetBIOS Name Server (NBNS) protocol, part of the NetBIOS over TCP/IP (NBT) family of protocols, is implemented in Windows systems as the Windows Internet Name Service (WINS). By design, NBNS allows network peers to assist in managing name conflicts. Also by design, it is an unauthenticated protocol and therefore subject to spoofing. A malicious user could misuse the Name Conflict and Name Release mechanisms to cause another machine to conclude that its name was in conflict. Depending on the scenario, the machine would as a result either be unable to register a name on the network, or would relinquish a name it already had registered. The result in either case would be the same – the machine would not respond requests sent to the conflicted name anymore.“ [MS00-047]

Gegenmaßnahmen

Wie in [MS00-047] beschrieben, sollten die verwendeten Ports nicht aus einem öffentlichen Netzwerk erreichbar sein und in der Firewall gesperrt werden (UDP Port 137). Ein interner Angreifer kann sich natürlich trotzdem diese Eigenschaft des NetBIOS-Protokolls zu Nutze machen.

4.2.4 Domain Name System (DNS)

Die Windows 2000 Domänencontroller verwenden das Domain Name System (DNS) für die Verwaltung der Domänenstruktur. Daher ist ein DNS-Server notwendig, um eine Windows 2000 Domänenstruktur zu betreiben, dieser speichert die Adressen der Server und der Arbeitsstationen. Der DNS-Server enthält auch Adressen für bestimmte Netzwerkressourcen, wie z.B. die Adresse des globalen Katalogs, Adressen für Kerberos- und LDAP-Dienste.
Die Verwendung von Dynamic DNS erlaubt die Veränderung von DNS-Daten durch DNS-Clients oder durch den DHCP-Server. Die Möglichkeit, DNS-Einträge über das Netzwerk zu verändern, kann weitere Sicherheitsprobleme erzeugen.

Preisgeben von Informationen über Domänen

Windows 2000 speichert viele sensible Daten im DNS. Dazu gehören die Adressen der Domänencontroller, der Clients und die Adressen verschiedener Dienste wie Kerberos oder LDAP. Diese Daten werden von Windows 2000 Clients benötigt und sollten daher auch nicht entfernt werden.

Ein Angreifer kann durch einen DNS-Server Adressen von Servern, Firewalls, Mailservern oder bestimmten Arbeitsstationen erhalten und für weitere Angriffe verwenden.
DNS-Server enthalten evtl. auch Informationen über öffentliche Domänen, wie z.B. die eigene Internetdomäne. Dann muss der DNS-Server aus dem Internet erreichbar sein, wodurch der Angreifer Zugriff erhält.
Durch einen Zonentransfer kann der Angreifer sogar alle Daten für eine Domäne in einem Stück vom DNS-Server erhalten und sich das mühsame Abfragen von einzelnen Ressourcen ersparen. Nur ein DNS-Server, der berechtigt ist eine Domäne zu übertragen (z.B. der DNS-Server des Internet-Providers), sollte in der Lage sein, einen Zonentransfer durchzuführen.

Gefahren

Da ein Angreifer sich normalerweise erst einmal einen Netzwerkplan des anzugreifenden Netzwerks erstellt, ist ein DNS-Server eine große Hilfe. So erhält er nicht nur eine Übersicht der Server und Arbeitsstationen, sondern auch Informationen über das verwendete Betriebssystem und verwendete private und öffentliche IP-Adressbereiche. Er kann daraus auf Computer schließen, die besondere Aufgaben haben (z.B. der Computer „Buchhaltung"), und welche Computer Kontakt zur Außenwelt haben (z.B. die Computer („MAIL", „FIREWALL" oder „INTERNET"). Da man es einem Angreifer nicht zu leicht machen sollte, muss der Zugriff auf solche Informationen verhindert werden.

Gegenmaßnahmen

Zuerst sollte festgestellt werden, ob der DNS-Server, der die Windows 2000 Domänenstruktur speichert, überhaupt aus einem öffentlichen Netzwerk zugänglich sein muss, dies wird nur in wenigen Fällen notwendig sein. Werden noch öffentliche Domänen gespeichert, so sollte dafür ein getrennter DNS-Server zur Verfügung stehen, so dass der Zugang aus dem Internet auf diesen Server mit den öffentlichen Domänen beschränkt werden kann.

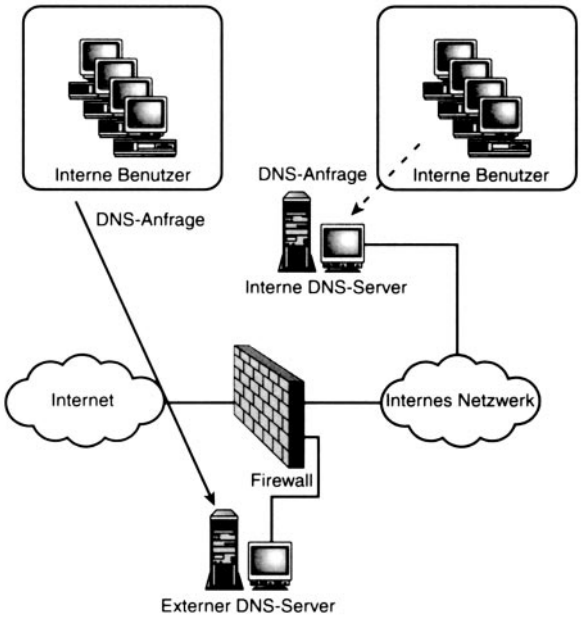

Abbildung 4-6 „Durch interne und externe DNS-Zonen kann die Sicherheit im Umgang mit DNS erhöht werden." [SCH01]

Damit ein Angreifer nicht die gesamten Daten einer Domäne auf einmal auslesen kann, sollten Zonentransfers nur für bestimmte IP-Adressen oder gar nicht freigegeben werden. Diese Einstellung kann und muss für jede Zone getrennt vorgenommen werden und verbirgt sich in den Eigenschaften einer Zone im DNS-Verwaltungsprogramm.

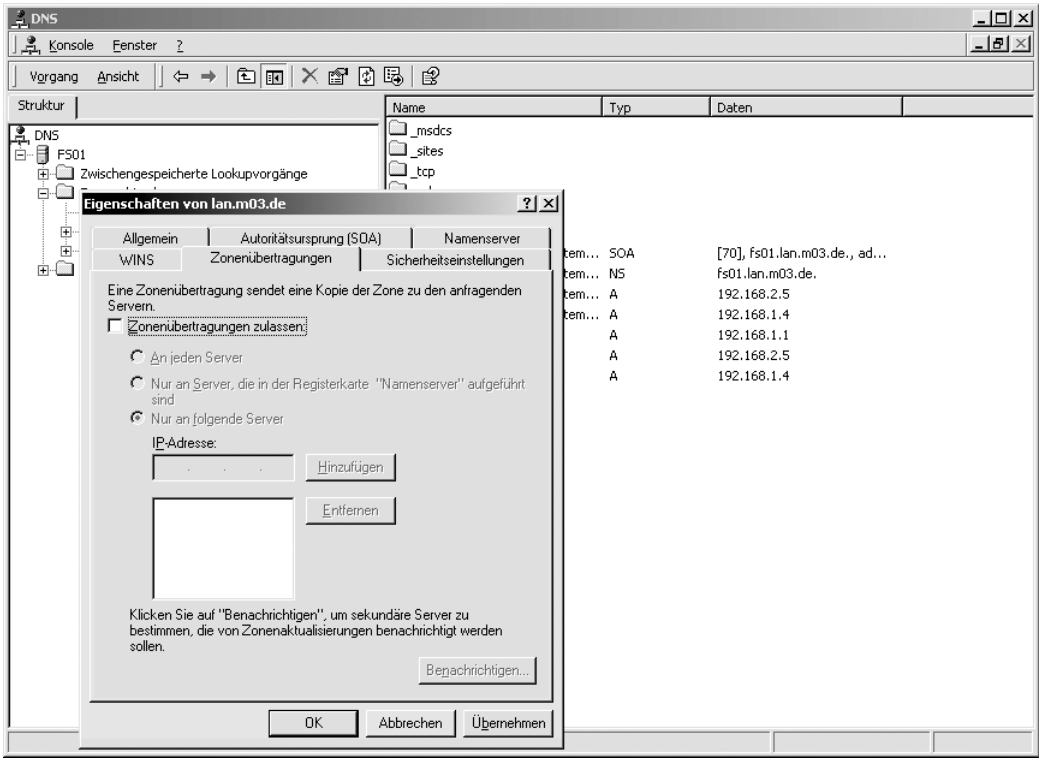

Abbildung 4-7 Zonentransfereigenschaften einer Domäne

Sind überhaupt keine Zugriffe von außen auf interne DNS-Server notwendig, was in den meisten Fällen zutrifft, so kann dies auch in der Firewall verhindert und Port 53 von außen gesperrt werden. Dabei verwenden normale DNS-Abfragen den UDP Port 53 und Zonentransfers wegen der Größe der übermittelten Daten den TCP Port 53.

Manipulation von DNS-Einträgen

Windows 2000 verwendet einen DNS-Server, der Veränderung der Einträge durch Clients gestattet (DDNS, Dynamic DNS). Wird ein Windows 2000 Client gestartet, bezieht er mit dem DHCP Protokoll eine IP-Adresse vom DHCP-Server und meldet seine IP-Adresse und seinen Namen am DNS-Server an. Domänencontroller ändern Einträge im DNS für Dienste wie Kerberos oder den globalen Katalog (GC), DHCP-Server können Clients eintragen, die nicht Windows 2000 verwenden.

Gefahren

Ein Angreifer kann nun versuchen, die Einträge im Domain Name System zu verändern. Gelingt es ihm eine neue IP-Adresse für einen Computer oder Dienst einzutragen, senden die Arbeitsstationen ihre E-Mails evtl. an einen fremden Mailserver und versuchen, auch dort neue E-Mails abzuholen, wofür sich die E-Mail-Clients mit ihrem Benutzernamen und Passwort anmelden.

Der Angreifer erhält so E-Mails und Passwörter, die er weiterverwenden kann. Dies ist natürlich nur ein Beispiel, ein Windows 2000 DNS-Server enthält noch viele interessante Einträge wie bereits weiter oben beschrieben.

Gegenmaßnahmen

Die dynamische Aktualisierung von DNS-Einträgen kann für jede Zone getrennt aktiviert werden. DNS-Zonen, die im Active Directory gespeichert sind, können so konfiguriert werden, dass nur gesicherte Aktualisierungen erlaubt sind. Einträge für diese Zonen werden im Active Directory gespeichert und durch DACLs gesichert. Die sichere dynamische Aktualisierung erfolgt dabei durch das in [RFC2078] definierte *Generic Security Service Application Programming Interface (GSS-API)* und verwendet Kerberos als Sicherheitsmechanismus. Die Aktivierung der gesicherten Aktualisierung erfolgt ebenfalls in dem Eigenschaftendialogfenster einer Zone.

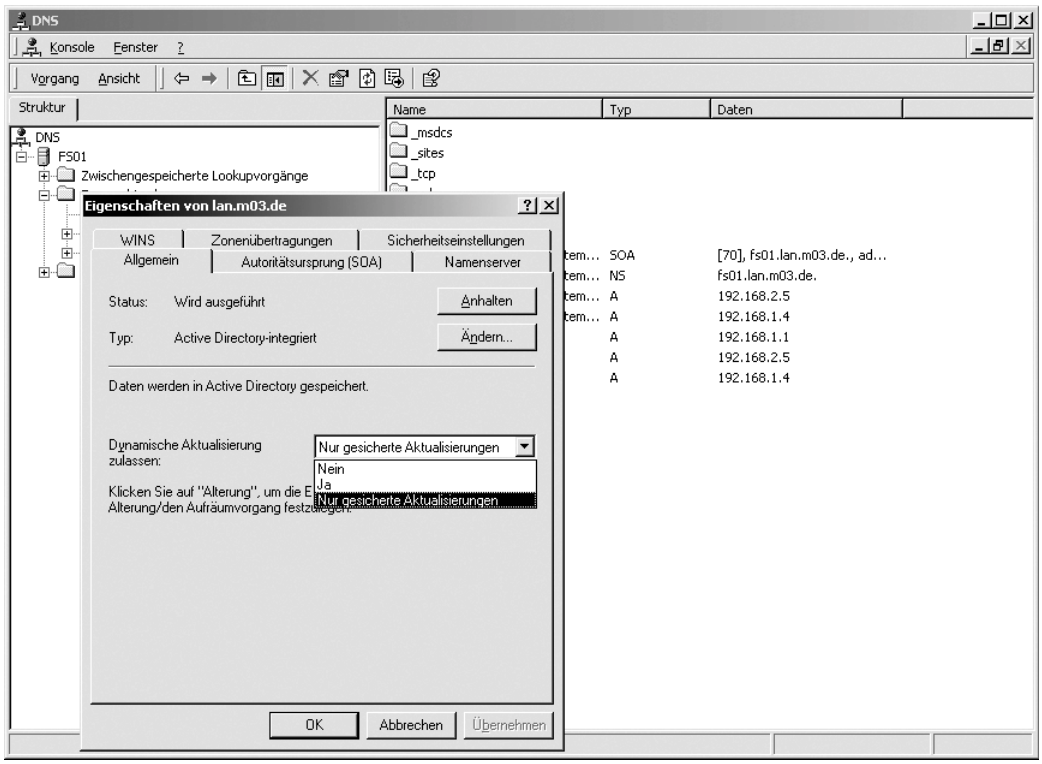

Abbildung 4-8 Aktivieren von gesicherten Aktualisierungen

Diese Sicherheitseinstellungen können allerdings nur für Zonen eingerichtet werden, die im Active Directory gespeichert sind. Andere Zonen unterstützen zwar auch eine dynamische Aktualisierung, diese wird aber nicht gesichert übertragen. Daher sollte diese Funktion für solche Zonen unbedingt deaktiviert werden, was sie normalerweise automatisch ist.
Ein Windows 2000 Client ist in der Lage, eine gesicherte Aktualisierung vorzunehmen oder diese durch den DHCP-Server zu veranlassen. Allerdings versucht der Windows 2000 DNS-Client zuerst eine ungesicherte Aktualisierung und wenn diese fehlschlägt wird er eine gesicherte Aktualisierung verwenden.

Da die gesamte DNS-Aktualisierung gesichert ablaufen sollte, kann diese Einstellung auch in der Registrierung geändert werden. Dazu muss folgender Wert hinzugefügt werden:

Schlüssel: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Name: UpdateSecurityLevel
Werte:
0 - zuerst ungesicherte Aktualisierung versuchen, dann gesicherte
16 - nur ungesicherte Aktualisierungen verwenden
256 - nur sichere Aktualisierungen verwenden

DNS-Antworten manipulieren

Fordert ein Client eine Adresse von einem DNS-Server an, muss sich dieser darauf verlassen, dass die Antwort wirklich vom DNS-Server stammt. Ist ein Angreifer in der Lage, einen DNS-Server durch einen DoS-Angriff auszuschalten, kann er sich unter Umständen als dieser ausgeben und falsche Antworten generieren. Es gibt Möglichkeiten mit einfachen Mitteln einen Windows 2000 Server, der nicht über die notwendigen Softwareupdates verfügt, kurz zu blockieren. Auch DNS-Anforderungen werden dann nicht mehr beantwortet. Der Angreifer kann einen anfragenden Client mit einer eigenen IP-Adresse versorgen.

Gefahren

Wenn ein Benutzer bspw. eine URL in einem Internetbrowser eingibt, vertraut er darauf, dass die Website wirklich die ist, deren URL er eingegeben hat. Wird ein DNS-Server so manipuliert, dass der Benutzer auf einer falschen Website landet, kann ein Angreifer dies ausnutzen, um Daten, wie Kreditkartennummern oder Passwörter vom Benutzer zu bekommen, indem er die eigentliche Website vortäuscht.

Gegenmaßnahmen

Damit DNS-Clients keine falschen Daten von einem DNS-Server erhalten, sollte dieser gegen DoS- oder andere Angriffe möglichst sicher sein. Dies kann durch Einstellungen und durch Softwareupdates geschehen. Wichtige DNS-Server sollten außerdem überwacht werden, damit ein Angriff zumindest möglichst früh erkannt wird. Windows 2000 kennt einige netzwerkbasierte DoS-Angriffe, die aber durch Installation der entsprechenden Updates behoben werden können

4.2.5 FileServer (Datei- und Druckerfreigabe)

Standardfreigaben von Laufwerken

Nach einer Installation von Windows 2000 sind alle vorhandenen Laufwerke für einen Administratorzugang vom Netzwerk freigegeben. Sie haben die Bezeichnungen C$ für Laufwerk C, D$ für Laufwerk D, usw. Alle bei einer Installation vorhandenen Partitionen werden auf diese Weise freigegeben, erscheinen allerdings nicht in der Netzwerkumgebung des Rechners, da aber jeder von diesen Standardfreigaben weiß, benutzen sie auch viele. Um sich mit ihnen zu verbinden braucht man beispielsweise im Windows-Explorer in der Adressleiste nur ‚\\zielrechner\c$' einzugeben und erhält nach Eingabe von Name und Passwort eines Administrators Zugriff.

Gegenmaßnahmen

In den Eigenschaften eines Laufwerks kann die Konfiguration der Freigaben vorgenommen werden. An dieser Stelle sollte man nur Freigaben einrichten, die benötigt werden.

Unsichere Freigaben von Laufwerken

Es ist natürlich sehr leichtsinnig Freigaben zu vergeben, bei denen ein Benutzer kein Passwort benötigt, um Zugriff zu dem Laufwerk zu erlangen. Freigaben auf dieser Ebene sind sehr leicht zu missbrauchen, da ein Angreifer sie bloß finden muss.

Gegenmaßnahmen

Man sollte nur Freigaben einrichten, die man benötigt, und für diese auch nur den notwendigen Benutzern den Zugriff mit Passwortschutz erlauben. In den Freigabeeigenschaften eines Laufwerks oder Ordners kann man einigen Benutzern auch nur Lesezugriff geben und anderen mehr Rechte einräumen.

Angriffe durch Null-Sessions

Ist auf einem Windows 2000 System Port 139 offen, so kann man als anonymer Benutzer so genannte Null-Sitzungen (Null-Sessions) aufbauen und vom System viele Informationen, wie Benutzer- und Gruppennamen, Netzwerkressourcen, Registrierungsschlüssel und noch einiges mehr, abfragen. Mit der Anwendung ‚net view' kann sich ein Angreifer beispielsweise alle Freigaben auf dem Rechner anzeigen lassen.

Gegenmaßnahmen

Es gibt eine Möglichkeit dies zu unterbinden; unter Verwaltung, Lokale Sicherheitseinstellungen, lokale Richtlinien, Sicherheitsoptionen, Weitere Einschränkungen für anonyme Verbindungen, sollte ‚Kein Zugriff ohne explizite anonyme Berechtigung' gewählt sein.

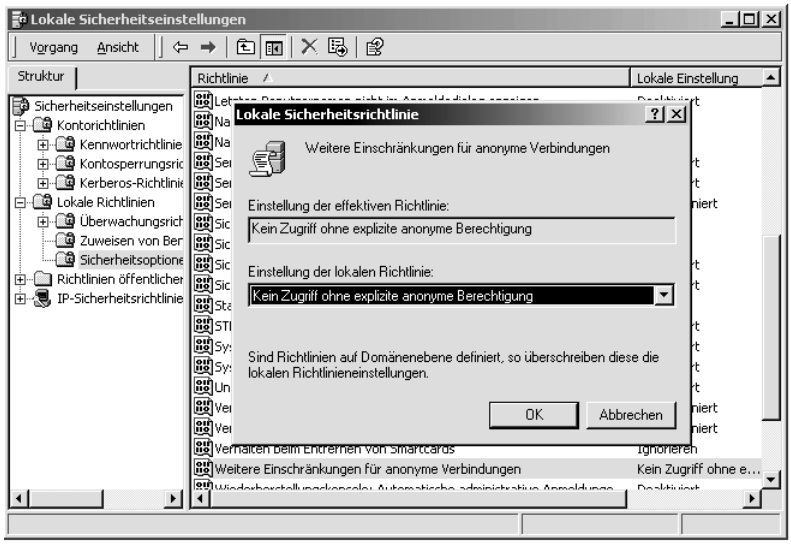

Abbildung 4-9 Lokale Sicherheitseinstellungen – Lokale Sicherheitsrichtlinie

Auf diese Weise kann die Einstellung, falls sie auf einem Domänencontroller in der Sicherheitsrichtlinie für Domänen vorgenommen wird, auch in einer Domäne weitervererbt werden. Alternativ kann man in der Registrierung mit ‚regedit.exe' unter HKLM\SYSTEM\CurrrentControlSet\Control\LSA im Menu Bearbeiten, Neu, Zeichenfolge folgendes eingeben

Name: RestrictAnonymous
Datentyp: REG_DWORD
Wert: 2

und danach den Registrierungseditor wieder schließen und den Rechner neu starten. Normalerweise sollte man die Ports 135 bis 139 und 445 sperren, wenn man sie nicht benötigt. Wenn Port 445 aktiv ist, kann ein Angreifer auf ein Windows 2000-System schließen.

Deaktivierung von SMB-Diensten durch Angriff

Laut [URL18] kann ein Angreifer SMB-Anfragen an Port 139 oder 445 senden, Antworten vom Server erhalten und diese jedoch nicht bestätigen. Daraufhin deaktiviert Windows 2000 alle auf SMB vertrauenden Dienste für 20 Sekunden und geht erst danach wieder an den Ports in den Abhörmodus. Dies kommt bei fortlaufendem Durchführen durch den Angreifer einem Denial-of-Service-Angriff auf SMB gleich.

Gegenmaßnahmen

Es sind keine Maßnahmen bekannt, um dies zu verhindern, außer die Ports zu sperren. Wenn man auf SMB angewiesen ist, hat man keine Möglichkeit dies zu unterbinden.

Appletalk-Authentifizierung überträgt Passwort nicht verschlüsselt

Bei einer Anmeldung von einem Apple Macintosh Rechner auf einem Windows 2000 Server mit Dateidiensten für Macintosh, wird das Kennwort unverschlüsselt übertragen. Somit ist das Kennwort über das Netzwerk abgreifbar.

Gegenmaßnahmen

Durch die Installation des UAM (User Authentification Module - Benutzerauthentifizierungsmodul) auf dem Apple Client, das im Verzeichnis ‚C:\Microsoft UAM-Datenträger' zur Verfügung steht, wenn Appletalk-Services installiert sind, kann man erreichen, dass das Kennwort verschlüsselt übertragen wird.

4.2.6 Internet Information Server (IIS) 5.0 und Active Server Pages (ASP)

Der IIS enthält die Internetdienste des Windows 2000 Betriebssystems. Als Webserver ist er beliebter Angriffspunkt für alle Angreifer und in den meisten Fällen aus dem Internet erreichbar. Aber auch die anderen Dienste, die der IIS zur Verfügung stellt, können Angriffen ausgesetzt werden. Sind die Dienste des IIS auf das Intranet beschränkt, gelten natürlich die gleichen Sicherheitsanforderungen, da Angriffe auch von internen Personen durchgeführt werden können. Diese Anforderungen sind normalerweise Vertraulichkeit und Integrität der Daten, sowie Zugriffskontrolle auf die Daten.

Durch die starke Integration des IIS in das Betriebssystem, ergeben sich neben den vielen Vorteilen für Entwickler auch Risiken, da ein erfolgreicher Angriff auf den IIS das gesamte System gefährden kann. Viele Dienste des IIS laufen im Sicherheitskontext des Systems, und gelingt einem Angreifer die Installation von Programmen oder Prozessen durch Sicherheitslücken im IIS, können diese unter Umständen die gleichen Rechte wie das Betriebssystem besitzen.

Integrität und Vertraulichkeit des Datenverkehrs und unerlaubter Zugriff auf Ressourcen

Die Sicherung des Datenverkehrs eines Webservers ist nur in den Fällen erforderlich, in denen es sich um vertrauliche Daten handelt. Der Großteil der öffentlichen Websites hat und benötigt keine Verschlüsselung, da sowieso jeder Zugriff auf die Daten hat.
Es gibt aber viele Anwendungen (z.B. E-Commerce, medizinische Anwendungen, Anwendungen im Intranet), die eine Verschlüsselung oder eine Authentifizierung des Servers oder des Clients benötigen.
Das HTTP-Protokoll stellt keine Methoden zur Verschlüsselung zur Verfügung und auch die integrierte Methode zur Authentifizierung ist eher ungenügend. Es bedient sich dazu anderer Protokolle, die diese Aufgabe übernehmen und diese Anforderungen erfüllen. Verwendung finden meistens SSL und TLS, die in vorhandene Webbrowser integriert worden sind.
Andere Protokolle, die der IIS verwendet, sind ähnlich aufgebaut. Während das häufig verwendete FTP-Protokoll nur eine Authentifizierung ermöglicht, die allerdings ungesichert übertragen wird, kann das SMTP- und NNTP-Protokoll ebenfalls SSL bzw. TLS verwenden und dadurch eine sichere Übertragung und Authentifizierung ermöglichen.
Der IIS muss außerdem gewährleisten, dass nur Daten verändert oder gelesen werden, für die der Benutzer eine Berechtigung hat. Der IIS stellt dazu eine Reihe von Werkzeugen bereit, um diese Zugriffe zu konfigurieren.

Gefahren

Werden vertrauliche Daten, wie Kreditkartennummern, von Dritten gelesen und verwendet, hat das weit reichende Konsequenzen für eine Website und ein Unternehmen.
Neben dem Verlust des Vertrauens in die Website werden Opfer evtl. Schadenersatzanforderungen stellen und der Betreiber muss sich gegenüber den Opfern verantworten.
News- und Mailserver haben allgemein noch nicht den Anspruch, sicher zu sein. Die meisten Benutzer von E-Mails finden es nicht oder nur wenig unerfreulich, dass diese in lesbarem Text über das Internet übertragen werden und von Angreifern gelesen werden können.
Wichtiger bei diesen Diensten ist die Authentifizierung, die aber eher beim Abholen von E-Mails eine Rolle spielt.
Die Authentifizierung bei den Web- und FTP-Diensten ist schon wichtiger, wenn z.B. eine Website oder FTP-Server nicht öffentlich zugänglich sein soll. Die Gefahren sind dann von den jeweiligen Anwendungen abhängig.
Die Veränderung von Daten auf dem Server darf natürlich nur ein Benutzer mit entsprechenden Rechten vornehmen, da dies ernste Folgen haben und zu erheblichen Schäden führen kann. Aber auch das Lesen von bestimmten Daten kann gefährlich sein, wenn diese sensible Informationen, wie Passwörter, enthalten.

Der IIS erlaubt auch das Ausführen von Programmen oder Scripten durch einen Benutzer und dieser Zugriff muss sorgfältig kontrolliert und darf nicht leichtsinnig vergeben werden. Wie leicht könnte sonst ein Befehl wie ‚FORMAT' oder ‚DROP DATABASE' großen Schaden am Dateisystem oder einer Datenbank anrichten oder Trojaner und Backdoors auf einem Server installieren.

Gegenmaßnahmen

Authentifizierung und Verschlüsselung wird durch verschiedene Protokolle den IIS-Diensten hinzugefügt. Einige dieser Protokolle sind weit verbreitet (z.B. SSL für Websites) andere werden jedoch kaum eingesetzt (z.B. SMTP-Authentifizierung) oder nicht vom IIS unterstützt (z.B. SSL für FTP-Verbindungen).
Für die Datenverschlüsselung wird in der Regel SSL/TLS verwendet, wobei der Einsatz von IPSec in Unternehmensnetzwerken ebenso möglich ist. Zur Authentifizierung können die Windows-Anmeldung oder aber auch Zertifikate und in Klartext übertragene Passwörter verwendet werden. Letzteres ist nur in Verbindung mit einer Verschlüsselung sinnvoll, da ansonsten die Passwörter unverschlüsselt übertragen und abgehört werden könnten.
Die Zugriffsrechte, die ein Benutzer über den IIS erhält, können durch verschiedene Einstellungen eingerichtet und beschränkt werden. Diese sollten sehr sorgfältig gewählt werden, gerade wenn der Server öffentlich zugänglich ist.

Authentifizierung

Die einzelnen Dienste, die der IIS anbietet, unterstützen unterschiedliche Methoden zur Authentifizierung. Die meisten Methoden verwenden allerdings Benutzernamen und Passwörter in Klartext oder sind auf bestimmte Browser oder das Windows Betriebssystem beschränkt.

HTTP-Authentifizierung

Der HTTP-Dienst kennt fünf verschiedene Methoden zur Authentifizierung, die unterschiedlich sicher und kompatibel zu verschiedenen Browsern sind.

- **Anonyme Authentifizierung**
  Wird die *anonyme Authentifizierung* verwendet, muss sich der Besucher nicht mit einem Namen und Passwort anmelden, sondern bekommt durch den IIS automatisch ein Benutzerkonto zugewiesen. Normalerweise ist dies das „IUSR_<computername>" Konto, das automatisch angelegt wird und Mitglied der Gruppe „Gäste" ist, wodurch der Zugriff auf das Dateisystem eingeschränkt wird. Der IIS übernimmt für dieses Konto die Kontrolle über das Passwort und kann dadurch anonyme Webbenutzer mit diesem Konto anmelden.
- **Standardauthentifizierung**
  Die *Standardauthentifizierung* verlangt vom Benutzer die Eingabe eines Namens und eines Passworts eines Windows 2000 Benutzerkontos, die unverschlüsselt übertragen werden. Der Benutzer wird dann mit diesem Konto am System angemeldet und erhält auch dessen Zugriffsrechte für z.B. das Dateisystem des Servers.
  Diese Anmeldung wird von fast jedem Webbrowser unterstützt, macht aber durch die unverschlüsselte Übertragung nur in Verbindung mit einem Verschlüsselungsprotokoll Sinn.

- **Digestauthentifizierung**
  Diese in [RFC2069] definierte Authentifizierung verwendet Hash-Werte für die Anmeldung an den Server. Der Server sendet eine entsprechende Anforderung an den Browser. Dieser fragt den Benutzer nach seinem Namen und seinem Passwort. Der Browser erstellt aus diesen Daten und der Serveranforderung einen Hash-Wert und sendet diesen an den Server. Der Server erstellt aus den lokalen Daten und der Anforderung ebenfalls einen Hash-Wert und vergleicht diese. Stimmen sie überein, wird der Benutzer angemeldet. Da diese Methode keine Benutzerdaten in Klartext überträgt, ist sie deutlich sicherer als die Standardauthentifizierung. Damit der Server einen Hash-Wert erzeugen kann, muss das lokale Passwort im Klartext bekannt sein und Windows 2000 verwendet eine reversible Verschlüsselung, um das Passwort zu speichern. Da diese die Sicherheit des Benutzerkontos beeinträchtigt, muss es explizit für das Benutzerkonto aktiviert werden. Da diese Form der Authentifizierung durch das IETF in einer RFC definiert wurde, wird es in Zukunft immer mehr Browser geben, die es unterstützen.
- **Windows-Authentifizierung**
  Diese Authentifizierung verwendet die normale Windows-Anmeldung, um einen Benutzer zu identifizieren und unterstützt die verschiedenen Windows-Anmeldeformen bis hin zum Kerberos-Protokoll. Dies stellt aus Sicht von Microsoft die sicherste Anmeldung dar, kann aber nur von kompatiblen Browsern (zur Zeit der Internet Explorer von Microsoft) verwendet werden. „Hierbei wird keine Benutzername/Kennwort-Kombination über das Netzwerk gesendet, sondern der Client muss im Rahmen eines kryptografischen Vorgangs nachweisen, dass er das Kennwort kennt“ [BRI01].
- **Zertifikatsauthentifizierung**
  Die Authentifizierung erfolgt anhand eines Clientzertifikats. Der Server überprüft mit Hilfe eines installierten Clientzertifikats die Identität des Benutzer. Diese Authentifizierung kann nur in Zusammenhang mit SSL/TLS verwendet werden. Für diese Anmeldung muss der Client über ein Clientzertifikat und der Server über ein Serverzertifikat verfügen. Die Clientzertifikate ordnet der Server entweder direkt einem Benutzerkonto zu (1:1 Zuordnung) oder der Server überprüft nur einige Daten im Zertifikat mit angegebenen Werten (n:1 Zuordnung). Der Benutzer muss kein Kennwort eingeben, sondern das Clientzertifikat bei einer Zertifizierungsstelle erwerben und dies in seinem Browser installieren.

Sowohl der WebDAV-Dienst und auch der IPP-Dienst verwenden HTTP als Basisprotokoll. Daher gelten die Authentifizierungsmethoden auch für diese Dienste.

FTP-Dienst

Der FTP-Dienst kennt nur die anonyme und die Standardauthentifizierung. Daher wird entweder kein Passwort verlangt oder dies unverschlüsselt im Netzwerk übertragen. Der IIS unterstützt auch keine weiteren Verschlüsselungen des Datenstroms auf der Anwendungsebene für das FTP-Protokoll, so dass eine wirklich sichere Authentifizierung für die FTP-Dienste nicht möglich ist ohne den Netzwerkdatenstrom durch Protokolle wie IPSec zu verschlüsseln.

NNTP- und SMTP-Dienst

Obwohl der SMTP-Dienst eigentlich nur zum Versenden von E-Mails verwendet wird, kann es trotzdem erforderlich sein, die Benutzer zu authentifizieren, wenn z.B. nicht jeder diesen Server verwenden darf. Auch für den News-Dienst kann eine Authentifizierung sinnvoll sein, da beide Dienste über öffentliche Netzwerke angesprochen werden können.
Diese Dienste können entweder die anonyme Authentifizierung, die Standardauthentifizierung oder die Windows-Authentifizierung verwenden und damit Passwörter bei der Standardauthentifizierung nicht in Klartext übertragen werden unterstützen sie die Verwendung von SSL/TLS zur Verschlüsselung der Daten und der NNTP-Dienst kann sogar Clientzertifikate verwenden.

Generell wird jedem Benutzer, der einen IIS-Dienst anfordert, ein Benutzerkonto zugeordnet. Durch die Klassifizierung von Windows NT 4.0 in die C2-Einstufung ist es erforderlich, dass jeder Benutzerzugriff authentifiziert wird. Auch wenn Windows 2000 noch nicht klassifiziert wurde, gelten diese Bedingungen und jeder Benutzer muss irgendwie authentifiziert werden.
Daher wird auch einem anonymen Benutzer ein Konto zugewiesen (normalerweise das „IUSR_<computername>"-Konto), damit der Zugriff auf Daten und Ressourcen über dieses Konto eingeschränkt werden kann.
Müssen sich Benutzer mit einem Namen und Passwort identifizieren, so sollten bei Verwendung der Standardauthentifizierung die Netzwerkdaten in irgendeiner Form verschlüsselt werden, damit die Passwörter nicht durch einfaches Abhören des Netzwerks gelesen werden können.

Zugriffsrechte

Damit die Benutzerauthentifizierung einen Sinn hat, muss der IIS feststellen können, welche Benutzer welche Zugriffsrechte haben. Der IIS verwendet mehrere Methoden zur Feststellung, ob ein Benutzer eine Ressource verwenden darf. Dabei hat eine restriktivere Einschränkung Vorrang gegenüber einer weniger restriktiveren.
Der IIS verwendet für Ressourcen, die im Dateisystem gespeichert sind, dessen Zugriffsmechanismen. Daher sollte ein Datenträger, der Ressourcen für den IIS bereitstellt, das NTFS-Format verwenden, da nur dort die Zugriffsrechte für einzelne Dateien und Benutzer wirkungsvoll konfiguriert werden können. Sie beziehen sich immer auf das Benutzerkonto, mit dem sich ein Benutzer am IIS angemeldet hat (für die anonyme Anmeldung wird das erwähnte „IUSR_<computername>"-Konto verwendet). Die NTFS-Rechte werden für das Lesen, Schreiben und auch das Ausführen von Dateien verwendet. Da ein Internetuser in der Lage ist, über den IIS und das HTTP-Protokoll auch Programme auszuführen, ist diese Einschränkung nicht unwesentlich. Insgesamt sind folgende Berechtigungen für Objekte im NTFS-Dateisystem einstellbar:

Berechtigung	Vollzugriff	Ändern	Lesen, Ausführen	Lesen	Schreiben
Ordner durchsuchen/ Datei ausführen	Ja	Ja	Ja	Nein	Nein
Ordner auflisten/ Daten lesen	Ja	Ja	Ja	Ja	Nein
Attribute lesen	Ja	Ja	Ja	Ja	Nein
Erweiterte Attribute lesen	Ja	Ja	Ja	Ja	Nein
Ordner/ Dateien erstellen	Ja	Ja	Nein	Nein	Ja
Attribute schreiben	Ja	Ja	Nein	Nein	Ja
Erweiterte Attribute schreiben	Ja	Ja	Nein	Nein	Ja
Unterordner und Dateien löschen	Ja	Nein	Nein	Nein	Nein
Löschen	Ja	Ja	Nein	Nein	Nein
Berechtigungen lesen	Ja	Ja	Ja	Ja	Ja
Berechtigungen ändern	Ja	Nein	Nein	Nein	Nein
Besitzrechte übernehmen	Ja	Nein	Nein	Nein	Nein
Synchronisieren	Ja	Ja	Ja	Ja	Ja

Tabelle 4-2 „Berechtigungen für Ressourcen" [SCH01]

Damit nicht für jede Ressource die NTFS-Rechte eingestellt werden müssen, besitzt der IIS noch eine weitere Methode, die Zugriffsrechte zu beschränken.
Diese werden direkt im Verwaltungsprogramm des IIS eingestellt und beziehen sich z.B. auf eine komplette Website oder ein virtuelles Verzeichnis. Dort können Rechte für das generelle Lesen und Schreiben eingerichtet werden, die der IIS durchsetzt. Soll ein Internetbesucher nicht die Möglichkeit haben, Verzeichnisse auf dem Server zu durchsuchen, kann dies ebenfalls für eine Website oder ein virtuelles Verzeichnis deaktiviert werden. Fordert ein Besucher ein Verzeichnis an, wird ihm eine Datei mit einem Standardnamen im Verzeichnis angezeigt, ist diese nicht vorhanden, wird eine Fehlermeldung zurückgegeben.

Script- und Programmzugriff

Der Webdienst des IIS gestattet es einem Benutzer, Programme oder Scripte auf dem Server auszuführen und das Ergebnis dann z.B. in Form einer Internetseite zu betrachten. Diese Funktion könnte dazu verwendet werden, Programme eines Angreifers oder Systemprogramme aufzurufen und auszuführen.
Die Vergabe dieser Rechte muss sehr sorgfältig geschehen. Hat ein Angreifer die Möglichkeit, in einem Verzeichnis zu schreiben und auch Programme auszuführen, dann ist er in der Lage, beliebige Programme auf den Server zu laden und diese zu starten, was unbedingt verhindert werden muss.

Scripte sind eine Form von Programmen, die erst von einer Servererweiterung übersetzt werden müssen. Der IIS unterscheidet daher zwischen dem Recht, ein Programm auszuführen und ein Script zu verwenden. Je nach Anwendung kann auf die Programmausführung verzichtet werden. Ein Script ist allerdings eine normale Textdatei, die auch gelesen werden könnte, wenn der IIS dies normalerweise nicht verhindern würde. Daher kann ein Besucher eine Scriptdatei nicht herunterladen, wodurch der Programmcode unsichtbar bleibt. Dieser Schutzmechanismus kann allerdings mit der Option „Scriptzugriff" deaktiviert werden.

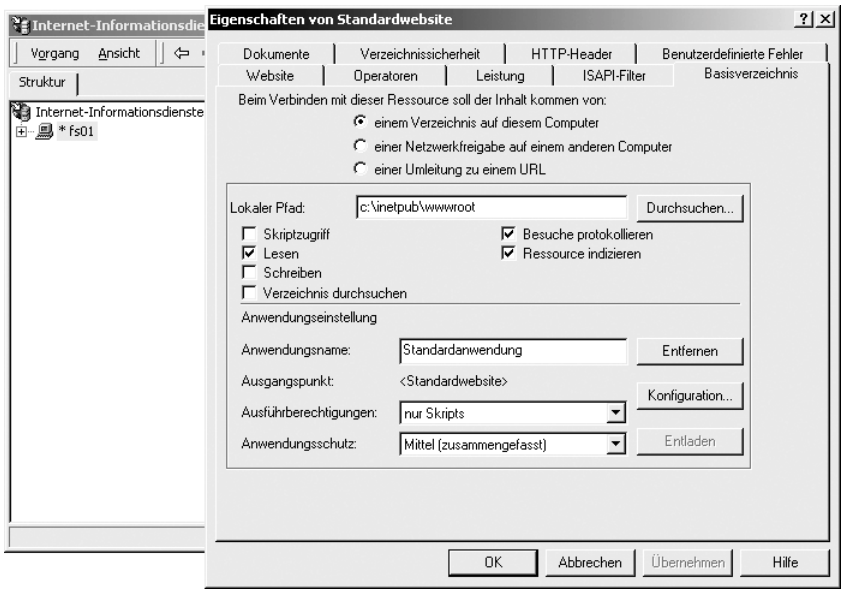

Abbildung 4-10 Einrichten der allgemeinen Zugriffsrechte einer Website

Die Einstellungen im NTFS-Dateisystem gelten für alle IIS-Dienste, daher auch für den FTP-Dienst. Auch er besitzt allgemeine Einstellungen, die für eine gesamte FTP-Site oder ein virtuelles FTP-Verzeichnis gelten. Der Administrator kann das Lesen und Schreiben insgesamt verbieten oder erlauben, die Ausführung von Programmen oder Scripten ist allerdings nicht über FTP möglich und muss auch nicht konfiguriert werden.

Zugriffsrechte für Netzwerkadressen

Der Zugriff auf die IIS-Dienste kann für bestimmte Netzwerkadressen verweigert oder erlaubt werden. Es können außerdem ganze Netzwerke oder Domänennamen für den Zugriff freigegeben oder gesperrt werden und diese Technik kann z.B. dafür eingesetzt werden, den Zugriff auf einen internen Webserver nur im Intranet zu erlauben. Durch die Möglichkeit, IP-Adressen zu spoofen, kann dieser Schutz allerdings evtl. umgangen werden. Die Absicherung interner Server durch eine Firewall ist ein zusätzlicher Schutz. Je mehr Sicherheitsbarrieren vorhanden sind, desto schwieriger wird es natürlich auch für einen Angreifer.

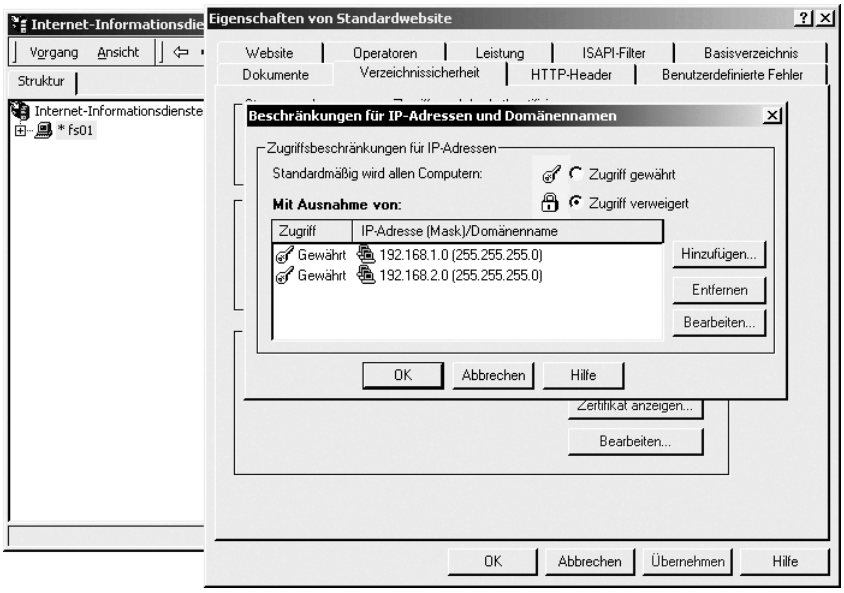

Abbildung 4-11 Einrichten der Beschränkungen für IP-Adressen

Verschlüsselung der Daten während der Übertragung

Für die Verschlüsselung der Daten während der Übertragung verwendet der IIS das SSL bzw. TLS Protokoll. Die Verschlüsselung wird für den HTTP- und den NNTP-Dienst angeboten oder kann auch auf Protokollebene mit IPSec erfolgen, sie ist dann mit allen Diensten verwendbar. Die IPSec Variante funktioniert meist nur in internen Netzwerken und nur mit Windows 2000 Clients.

SSL und TLS

Soll für die Verschlüsselung der Daten SSL bzw. TLS verwendet werden, ist ein Serverzertifikat erforderlich. Dies wird für den entsprechenden Dienst von einer Zertifizierungsstelle angefordert und im Server installiert. Die einzelnen Dienste können dann den Datenstrom mit Hilfe eines Sitzungsschlüssel verschlüsseln und nur der Client ist in der Lage, diese Daten zu entschlüsseln. Als Beispiel für die Einrichtung und Funktionsweise für die Verschlüsselung wird dies am HTTP-Dienst im folgenden erklärt.

Die Anforderung eines Serverzertifikats für eine Website wird durch den Zertifikatsassistenten erstellt. Dafür sind Angaben über den Zertifikatsinhaber und über die Website erforderlich. Diese Anforderung wird dann per E-Mail oder über ein Webinterface an eine Zertifizierungsstelle geschickt, die den Antrag prüft und nach positiver Überprüfung ein Serverzertifikat ausstellt, das mit dem privaten Schlüssel der Zertifizierungsstelle signiert wird.

Die Installation des neuen Zertifikats erfolgt ebenfalls mit Hilfe des Zertifikatsassistenten. Danach kann diese in den Einstellungen zur Verzeichnissicherheit diese bearbeitet werden.

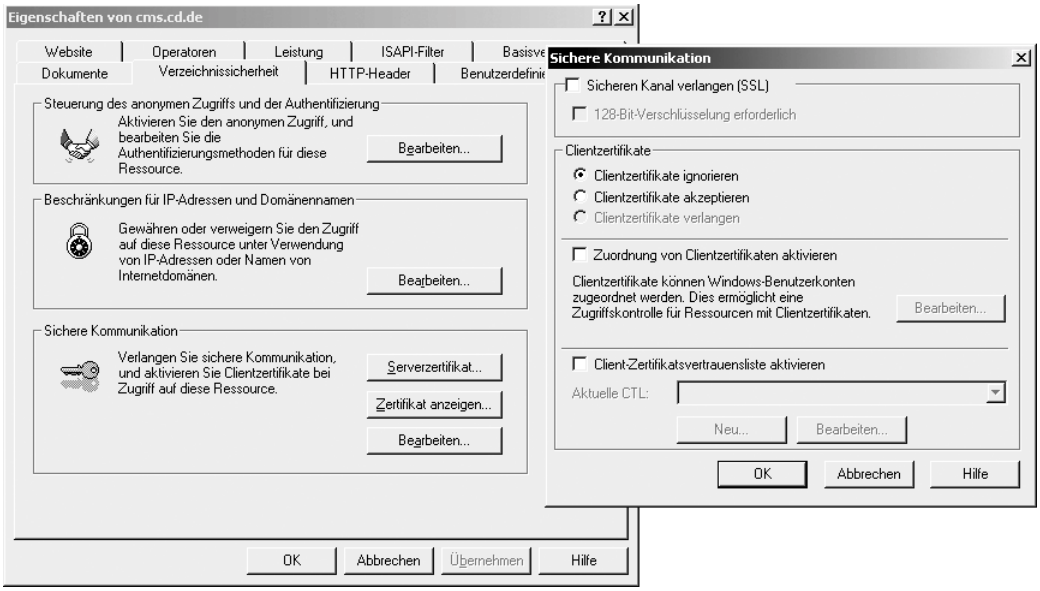

Abbildung 4-12 Einstellungen für eine sichere Verbindung

Dort kann die Verschlüsselung aktiviert und eingerichtet werden und es wird die minimale Verschlüsselungsstärke eingestellt. Durch die Lockerung der Exportbestimmungen der USA kann die Option ‚128-Bit-Verschlüsselung erforderlich' angewählt werden, wobei das High Encryption Pack auf dem Server installiert sein muss, das auch in Service Pack 2 enthalten ist. Sind nur 128 Bit Verschlüsselungen erlaubt, werden Anforderungen, die dies nicht ermöglichen, abgelehnt.
Die Einstellungen für die Clientzertifikate ermöglichen eine sichere Authentifizierung von Clients durch Zertifikate, die im Clientbrowser installiert sein müssen.
Wird eine Anforderung für eine sichere Verbindung an den HTTP-Server gesendet (HTTPS-Anforderung), sendet dieser sein Serverzertifikat mit seinem öffentlichen Schlüssel und der Client kann eine SSL-Verschlüsselung aufbauen. Die Verwendung von SSL/TLS und Zertifikaten erfordert allerdings zusätzliche Sicherheitsmaßnahmen, die im Kapitel 4.1.9 erläutert werden.

IPSec

Wird der Netzwerkverkehr auf Protokollebene durch IPSec verschlüsselt, ist eine SSL/TLS Verschlüsselung der Daten nicht erforderlich. IPSec kann nicht mit allen Plattformen verwendet werden und ist daher nur für Intra- bzw., Extranet-Anwendungen interessant. Dieser Umstand kann sich allerdings in Zukunft ändern, wenn IPSec eine größere Verbreitung findet.

Bekannte Sicherheitsprobleme

Fehlerhafte Ausgabe von Zertifikaten durch VeriSign Inc.

Wie das Unternehmen Microsoft in seinem Security Bulletin (MS01-017) geschrieben hat, sind zwei Zertifikate von VeriSign Inc. mit dem Firmennamen „Microsoft Corporation" an eine Person, die nicht zu Microsoft gehört, ausgegeben worden. Das Kapitel 4.1.9 enthält weitere Informationen hierüber.

Abhören von fremden Session ID Cookies

Der IIS verwendet Cookies, um einem Benutzer eine Session zuzuordnen. Diese Cookies werden in Klartext übertragen und können im Netzwerk abgefangen werden. Wird eine Übertragung verschlüsselt, verwenden ASP-Seiten das gleiche Cookie für verschlüsselte und unverschlüsselte Seiten und unterstützen keine sicheren Session ID Cookies, wie in [RFC2109] definiert. Wird eine gesicherte Verbindung aufgebaut und eine ungesicherte Seite übertragen, wird das Cookie diesmal unverschlüsselt übertragen und ein Angreifer kann es verwenden, um die Session des Benutzers zu übernehmen.
Microsoft hat dieses Problem in seinem Security Bulletin unter der Nummer MS00-080 beschrieben und einen Patch zur Verfügung gestellt, der das Problem behebt. Durch den Patch verwenden gesicherte Seiten die in [RFC2109] definierten Secure ID Cookies.

Ausfall des IIS oder des gesamten Systems

Ein typischer Angriff auf ein System ist eine DoS-Attacke, die in verschiedenen Formen auftaucht. Besonders wirksam sind verteilte Angriffe (DDoS), da viele angreifende Computer daran beteiligt sind.
Auch der IIS kann durch DoS-Angriffe ausfallen, wobei zwischen DoS-Angriffen, die Programmierfehler verwenden, und solchen, die durch extrem viele Anfragen die Bandbreite der Serveranbindung aufbrauchen, unterschieden werden muss. Natürlich hat jeder Server eine gewisse Leistungsgrenze, die erreicht werden kann. Interessant sind daher DoS-Angriffe, die Programmierfehler ausnutzen.

Gefahren

Wird ein IIS-Dienst wirksam angegriffen, kann es passieren, dass der Dienst beendet wird und neu startet; es kann auch der gesamte IIS ausfallen. Dann sind auch Programme und Dienste betroffen, die den IIS benötigen, wie z.B. Microsoft Exchange, unter Umständen kann auch das komplette System davon betroffen werden.
Normalerweise kann solch ein Absturz durch das Neustarten des Systems oder des Dienstes wieder behoben werden, so dass sich der Schaden auf die Nicht-Erreichbarkeit beschränkt.

Gegenmaßnahmen

Sollte der DoS-Angriff Programmierfehler verwenden, kann dies durch die Installation von existierenden Updates evtl. behoben werden. Ein Server kann auch so konfiguriert werden, dass er selbst neu startet, sobald ein Dienst nicht mehr funktioniert. Ein Angreifer kann aber evtl. genau das wollen, um vorher überspielte Software zu installieren.

Bekannte Sicherheitsprobleme

Fehlerhafte HTTP-Anforderung

Besonders einfach wird es für einen Angreifer, wenn ein DoS-Angriff über eine HTTP-Anforderung ermöglicht wird. Dann wird meistens auch eine Firewall das System nicht schützen können, da diese die entsprechende HTTP-Anforderung meist zulässt. Der IIS kennt einige solcher DoS-Angriffe, die den Server auslasten oder zum Abstürzen bringen. Microsoft hat diese im Security

Bulletin aufgenommen. Die Artikel MS00-23, MS00-30, MS00-044, MS00-100, MS01-014 und MS01-016 beschreiben diese Angriffe. Dabei findet ein Angriff über den WebDAV-Dienst statt und erzeugt eine extrem hohe Prozessorauslastung, ein anderer bringt den IIS durch eine fehlerhafte Anfrage an eine FrontPage-Erweiterung zum Absturz. Solche Probleme können vermieden werden, wenn unbenötigte Dienste nicht installiert werden oder die entsprechenden Softwareupdates installiert werden.
Auch MS01-026 beschreibt einen Programmfehler, der für einen DoS-Angriff auf dem FTP-Server verwendet werden kann und MS01-041 beschreibt ein Problem, durch das ein Angreifer mit bestimmten RPC Anforderungen verschiedene Dienste auf dem Server durch DoS-Angriffe blockieren kann. Dieses kann durch eine entsprechend konfigurierte Firewall verhindert werden, die keine RPC Anfragen durchlässt.
Microsoft hat zu allen bekannten Problemen Softwareupdates zur Verfügung gestellt, die teilweise in Service Pack 2 integriert sind. Es empfiehlt sich dringend, diese zu installieren.

Unerlaubtes Lesen von Scriptdateien (z.B. ASP)

Websites können Scripte enthalten, die von einem Besucher aufgerufen werden und ein Ergebnis als Antwort zurückgeben. Normalerweise ist der eigentliche Programmcode eines Scripts für den Internetbesucher nicht lesbar. Dieses Verhalten des IIS kann sich bei einem Fehler ändern.

Gefahren

Scripte können alle möglichen Informationen enthalten, die ein Angreifer nicht sehen darf. Sogar Passwörter von Datenbanken können in solchen Scripts enthalten sein, auf die ein Angreifer dann Zugriff hätte. Scripte können auch auf andere Schwachstellen oder Kommentare von einem Angreifer durchsucht werden, die dieser dann ausnutzen kann. Natürlich können Scripte so erstellt werden, dass kein Angreifer damit etwas anfangen könnte, selbst wenn er den Programmcode sehen kann. Diese Methode bietet die größte Sicherheit, wird aber nur selten umgesetzt.

Gegenmaßnahmen

Scriptdateien sollten möglichst wenige Informationen enthalten, die ein Angreifer verwenden kann, um die Gefahr von Anfang an zu minimieren. Der IIS bietet die Option „Scriptzugriff", die den Lesezugriff auf ein Script ermöglicht. Es ist klar, dass diese Option nicht aktiviert werden sollte, wenn sensible Daten in einem Script enthalten sind. Eine weitere Möglichkeit besteht darin, den Programmcode entweder zu verschlüsseln, ASP und der IIS 5.0 bieten diese Möglichkeit, oder mit einem Compiler in eine Library (DLL) zu verwandeln. Diese kann dann irgendwo im Dateisystem liegen und wird durch ein Script aufgerufen. Selbst wenn die Library erbeutet wird, muss sie zuerst zurückentwickelt werden, was den Aufwand erhöht. Einige Fehler im IIS 4.0 dieser Art wurden durch die installierten Beispiele verursacht, diese werden auf einem Produktionssystem nicht benötigt und sollten entfernt werden. Wird ein NT 4.0 System auf Windows 2000 aktualisiert, werden diese Beispiele nicht entfernt und stellen evtl. weiterhin eine Gefahr dar.

Bekannte Sicherheitsprobleme

Der IIS 4.0 hatte mit einigen Problemen zu kämpfen, die es ermöglichten, durch eine veränderte URL ein Script zu lesen. Auch der IIS 5.0 kennt diese Probleme. So empfiehlt Microsoft im Security Bulletin MS01-004 das Entfernen der „.htr"-Erweiterung, wenn diese nicht verwendet wird oder

die Installation des entsprechenden Updates. Auch MS00-044 und MS00-031 enthalten Informationen über Fehler dieser Art.
MS00-058 beschreibt ein ähnliches Problem, das durch einen fehlerhaften HTTP-Header ausgelöst wird. Auch in diesem Fall wird ein Script nicht verarbeitet, sondern einfach an den Browser gesendet. Grund scheint die WebDAV-Erweiterung zu sein, wie in [KUR01] behauptet wird: „Im Dialog mit dem Microsoft Produkt Sicherheits-Team konnten wir klären, dass es sich tatsächlich um ein WebDAV-Problem handelt, wobei WebDAV als ISAPI-Filter unter dem Namen httpext.dll implementiert wurde, der Web-Anforderungen vor dem Kern der IIS-Engine interpretiert." [KUR01]
Microsoft hat für diese Probleme Softwareupdates veröffentlicht, die auf der Microsoft Website heruntergeladen werden können.

Manipulation von Internetseiten

Neben dem unerlaubten Lesezugriff auf Ressourcen besteht auch die Gefahr, dass Ressourcen auf dem Server geändert oder geschrieben werden. Ein Angreifer könnte dann Programme oder Daten auf einem Server schreiben, um diese dann auszuführen.

Gefahren

Die Veränderung von Ressourcen auf einem Webserver kann lange unbemerkt bleiben, z.B. die Veränderung einer Internetseite in einer umfangreichen Website. Änderungen an Internetseiten können illegale Inhalte enthalten, für die der Eigentümer der Website verantwortlich gemacht werden könnte. Dies kann auch den Verlust von Vertrauen der Kunden oder Besucher zur Folge haben.
Kann ein Angreifer Inhalte manipulieren, ist er vielleicht auch in der Lage, Weiterleitungen auf eigene Websites einzusetzen und kann sensible Daten von Besuchern erbeuten, die davon ausgehen, sich noch auf der eigentlichen Website zu befinden.
Viele Websites bieten die Möglichkeit, eigene Inhalte zu publizieren. Dies geschieht in Form von Gästebüchern oder Foren. Ein Angreifer kann solche Bereiche nutzen, um eigenen Programm- oder Scriptcode in einer Seite zu plazieren, der dann auf dem Server oder in einem fremden Webbrowser ausgeführt wird. Auch auf diesem Wege können Weiterleitungen oder Frames erzeugt werden, die der Angreifer verwenden kann.

Gegenmaßnahmen

Grundsätzlich sollten alle Zugriffsrechte auf einem öffentlichen Server überprüft werden. Kein unbekannter Besucher sollte Schreibrechte bekommen und wenn Besucher Gästebücher o.ä. verwenden können, muss der Inhalt auf Scripte oder Programmcodes kontrolliert werden, eine inhaltliche Kontrolle ist außerdem sinnvoll.

Bekannte Sicherheitsprobleme

Die mögliche Einbindung von Scripten in Websites durch die Eingabe von Internetusern wird im Microsoft Security Bulletin MS00-060 beschrieben. Einige Microsoft-Produkte scheinen nicht jede Benutzereingabe zu kontrollieren, diese Fehler sollen aber durch das in MS00-060 beschriebene Softwareupdate behoben werden. „The vulnerability can affect any software that runs on a web server, accepts user input, and blindly uses it to generate web pages. Microsoft recommended that all vendors check their products to see if any are affected by the vulnerability, and initiated a

check of its own products as well. Several features in IIS were found to be affected – some were found by Microsoft internal teams, and others were identified by customers – and this patch eliminates all of them." [MS00-060]

Unerlaubtes Ausführen von Programm- oder Scriptcode

Die Veränderung von Ressourcen ist eine Möglichkeit, um Programme auf dem Server zu installieren. Neben diesen Möglichkeiten gibt es noch eine weitere, um eigenen Programmcode auf einem Server auszuführen: der Pufferüberlauf. Wird ein solcher Fehler entdeckt und ausgenutzt, kann das katastrophale Folgen haben. Der Programmcode wird dann evtl. im Sicherheitskontext des angegriffenen Dienstes ausgeführt und da der IIS als Dienst vom System gestartet wird, kann ein feindliches Programm hohe Zugriffsrechte bekommen.
Durch Programmierfehler können auch Situationen entstehen, in denen die Grenzen des Hauptverzeichnisses einer Website überschritten werden und gegebenenfalls Systemprogramme von einem Angreifer verwendet oder verändert werden können. Ist der Zugriff auf solche Programme durch einen Programmfehler im IIS möglich, ist auch nicht mehr gewährleistet, dass die Ausführung verhindert wird.

Gefahren

Ein Angreifer, der in der Lage ist Programmcode auf dem Computer auszuführen, kann großen Schaden anrichten. Die Installation von Trojanern, Backdoors und Würmern ist nur eine Möglichkeit, die er verwenden kann. Er ist dann evtl. in der Lage, Daten zu manipulieren oder Passwörter zu erbeuten und er kann diesen Zugang auch dazu nutzen, weitere Computer im Netzwerk anzugreifen. Dabei ist die Gefahr von Pufferüberläufen besonders kritisch, da die betroffenen Dienste meist mit hohen Zugriffsrechten ausgestattet sind.

Gegenmaßnahmen

Die Gefahren durch Pufferüberlaufe in einem Webserver können eigentlich nur wirksam von den Entwicklern behoben werden, sei es Microsoft oder ein Entwickler einer installierten Software. Daher sollten aktuelle Softwareupdates zumindest überprüft und dann installiert werden.
Andere Probleme können auch selbst verursacht worden sein, da der IIS durchaus die Installation und Ausführung von Software gestatten kann, wenn diese Rechte explizit eingeräumt werden. Ein Besucher sollte nie in der Lage sein, Dateien auf einen Server übertragen zu können und dann die Möglichkeit haben, solche Dateien auszuführen.
Das Windows 2000 Betriebssystem bietet außerdem gute Überwachungsmöglichkeiten, womit sich das Ausführen von Programmen aufzeichnen lässt.

Bekannte Sicherheitsprobleme

Die momentan berühmteste Schwachstelle dürfte der Pufferüberlaufs-Fehler in der „idq.dll" sein, die vom IIS für den Indexdienst verwendet wird und den Code Red-Wurm und seine Nachfolger ermöglicht hat. Obwohl dieser Fehler von Microsoft im Security Bulletin Dokument MS01-033 am 18.Juni veröffentlicht wurde und ein Softwareupdate für diesen Fehler vorhanden ist, das die Infektion eines Servers verhindern kann, wurden sehr viele Computer mit dem Wurm infiziert, was auf ein niedriges Interesse an Serversicherheit schließen lässt.

Es existieren auch andere Schwachstellen wie z.B. der Pufferüberlaufsfehler in der Erweiterung für den IPP-Druckdienst des IIS. Der Fehler wird in MS01-023 beschrieben und ein Softwareupdate ist vorhanden und in Service Pack 2 integriert. Wird der IPP-Druckdienst nicht verwendet, kann die ISAPI Erweiterung auch deinstalliert werden.
Andere Probleme sind in MS00-086 und MS00-078 beschrieben. Betroffen sind die Überprüfungen von Zugriffen auf Programme und Zugriffe auf Verzeichnisse außerhalb der Webverzeichnisse. Angreifer können damit Systemprogramme ausführen und verwenden. Für beide Probleme sind Softwareupdates vorhanden, die in Service Pack 2 integriert sind.
Das Dokument MS01-026 beschreibt die Möglichkeit, dass ein Angreifer eigenen Programmcode auf den IIS ausführen kann und liefert ein Update, um das Problem zu beheben. Dieses Update wird allerdings erst in Service Pack 3 integriert sein und muss als einzelnes Update installiert werden.

4.2.7 Terminaldienste

Der Terminaldienst kann für die Remoteverwaltung des Servers oder als Anwendungsserver konfiguriert werden. In beiden Fällen wird er dazu verwendet, Programme lokal auf dem Server und nicht auf dem Client auszuführen und die Ergebnisse in Form einer grafischen Oberfläche zurückzugeben.
Gerade zur Administration eines Servers sind solche Dienste überaus praktisch, geben aber potentielle Angreifer ein ebenso wertvolles Instrument in die Hand, falls ein Zugang zum Server möglich ist. Die Terminaldienste verwenden zur Übertragung nur einen einzigen Netzwerkport (Port: 3389) und können daher gut in einer Firewall gesichert werden. Der Zugriff kann natürlich auch gewollt über öffentliche Netze erfolgen. Dann sichert eine eingebaute Verschlüsselung die übertragenen Daten.
Verwendete Sitzungen können zentral überwacht und auch verfolgt werden, was das Überprüfen von Zugängen erleichtert und selbst ein erfolgter Zugang setzt noch die Anmeldung am System mit einem Benutzerkonto voraus, das über entsprechende Zugriffsrechte verfügt.

Übernahme einer abgebrochenen Verbindung

Wird eine Verbindung zu einem Terminalserver hergestellt, muss sich der Benutzer trotzdem noch mit einem Benutzerkonto anmelden. Dieses Verfahren ist gleichzusetzen mit der direkten Anmeldung am Server. Genauso, wie sich ein Benutzer am Server anmeldet, muss er sich auch wieder abmelden. Wird eine Sitzung unterbrochen (z.B. wenn eine Internetverbindung zusammenbricht), wird der Benutzer normalerweise nicht automatisch abgemeldet. Ist ein Benutzer nicht mehr mit dem Server verbunden, besteht die Sitzung weiter.

Gegenmaßnahmen

Genauso wie eine lokale Sitzung am Server, sollte sich ein Terminalbenutzer immer abmelden, wenn er die Verbindung beendet oder diese unterbrochen wird. Der Terminalserver kann so konfiguriert werden, dass Benutzer automatisch abgemeldet werden, wenn die Sitzung unterbrochen oder beendet wird. Dies kann sofort oder nach einem Zeitlimit geschehen. Allerdings werden auch alle aktiven Prozesse bei solch einer Abmeldung beendet und es kann zu Datenverlust kommen.

Abhören der Daten während einer Terminalsitzung

Da sich ein Benutzer über die Terminalverbindung am Server anmelden muss, muss er auch sein Passwort eingeben, und diese Daten werden über das Netzwerk übertragen. Damit sie nicht abgehört und entziffert werden können, werden sie verschlüsselt übertragen.

Gegenmaßnahmen

Die Verschlüsselung der Daten erfolgt in drei verschiedenen Stufen. Die niedrige Sicherheitsstufe verschlüsselt nur Daten, die vom Client zum Server gesendet werden und verwendet dazu eine 40 Bit (Windows 9x Clients) bzw. eine 56 Bit (Windows 2000 Clients) Verschlüsselung.
Die mittlere Sicherheitsstufe verwendet die gleiche Verschlüsselungsstärke, diese wird in beide Richtungen eingesetzt.
Die hohe Sicherheitsstufe verschlüsselt die Daten mit einer 128 Bit Verschlüsselung in beide Richtungen. Für diese Einstellung muss das High Encryption Pack bzw. Service Pack 2 auf dem Server installiert sein. Für die Remoteverwaltung eines Domänencontrollers ist die hohe Sicherheitsstufe sicherlich die einzige Alternative, auch wenn die Verschlüsselung leicht zu Lasten der Performance geht.

Ausfall des Terminalservers

Der Terminalserver kann, wie jeder andere Dienst, der über das Netzwerk erreichbar ist, für DoS-Attacken empfänglich sein. Fällt der Terminalserver aus, kann auch kein Remotezugriff mehr auf den Server erfolgen, so dass sich die Behebung des Problems verzögern wird, da der Administrator direkt am Server tätig werden muss. Je nach Verwendung des Servers, kann so etwas den Arbeitsablauf erheblich stören.

Gegenmaßnahmen

Wie bei allen Problemen mit DoS-Angriffen, kann der Netzwerkzugriff eingeschränkt werden. Findet keine Administration des Servers über das Internet statt, sollte dieser Zugang verhindert werden. Außerdem sollten Softwareupdates, die dieses Problem betreffen, installiert werden, wenn diese verfügbar sind.

Bekannte Probleme

Das Microsoft Dokument MS01-006 beschreibt tatsächlich die Möglichkeit einer DoS-Attacke auf einen Terminalserver durch fehlerhafte RDP-Pakete. Dafür muss der Angreifer keine Sitzung öffnen, sondern lediglich entsprechende Pakete an den Server schicken. Der Dienst kann allerdings nach einem Neustart wieder verwendet werden. Ein Softwareupdate für dieses Problem ist vorhanden und in Service Pack 2 integriert.
Auch in MS01-040 wird ein solches Problem beschrieben. Der beschriebene Angriff hat einen Ausfall des Terminalservers und weiterer Dienste zur Folge und kann nur durch einen Neustart des Servers behoben werden. Ein Patch ist auf der Microsoft Website vorhanden.

5 Vermeidung von Sicherheitsproblemen

Ein sicheres Computersystem muss gut geplant sein. Es sollte dafür eine *Security Policy* geben, für Webserver ist ein Grundbaustein das [RFC2196] – „The Site Security Handbook". Es ist sehr wichtig, eine Security Policy zu haben, da man im Falle eines Zwischenfalls dann sofort ein Handbuch für das weitere Vorgehen zur Verfügung hat. In der Erstellungsphase macht man sich Gedanken über alle Arten von Zwischenfällen, die Auftreten können, und überlegt sich Gegenmaßnahmen. Dazu können auch das Trennen der Netzwerkleitungen nach außen oder das Herunterfahren der Systeme gehören, wenn man seine Daten zu schützen hat und ein Eindringling Zugang zum System erlangt hat. Entscheidend ist auch die Security Policy mit der Zeit an die Bedürfnisse und Veränderungen im Unternehmen anzupassen, immer über neue Sicherheitsprobleme informiert zu bleiben, z.B. durch Literatur, das Abonnieren von einschlägigen Newsgroups und Mailing-Listen und durch Informationen von den Herstellern der eingesetzten Produkte. Diese Informationen müssen in Form von Änderungen in die Security Policy eingehen und sie auf einem hohen Sicherheitsniveau, das von Anfang an bestehen sollte, halten.

Man sollte in Erwägung ziehen, sein System in festen Zeitabständen von unabhängigen, vertrauenswürdigen Dritten auf Sicherheitslücken und die Funktionalität der Security Policy hin überprüfen zu lassen. Hierbei kommen oft so genannte „Tiger-Teams" zum Einsatz, die zwar nicht sehr günstig arbeiten, dafür aber Spezialisten auf ihrem Gebiet sind und unterschreiben müssen, dass die eventuell erbeuteten Daten nicht durch sie verwendet werden. Dabei gibt es zwei Vorgehensweisen:
1.Der *Black-Box-Approach:* Man führt Netzwerkpenetration mit Port-Scannern, Sniffern und weiteren unter anderem in Kapitel 3 genannten Tools wie z.B. dem ‚SATAN'-Tool durch. Dieses Vorgehen verifiziert nur das Funktionieren der Firewalls und der einbruchsverhindernden Systeme.
2.*White-Box-Audit:* Hierbei wird von der Seite der Security Policy her untersucht, ob die Planung einwandfrei war. Dies geschieht meist mit Hilfe der involvierten Mitarbeiter und dabei können diese auch eine Menge von den Spezialisten lernen. Abschließend werden meist noch einige Praxistests durchgeführt, um eventuell übersehene Planungsfehler aufzudecken.
Die zweite Methode ist der ersten auf jeden Fall vorzuziehen, da sie einen viel größeren Bereich abdeckt, viel mehr Seiten in Betracht zieht und das System praxisgerecht testet, so wie es ein Angreifer tun würde.

Ein Thema, das an dieser Stelle natürlich nicht fehlen darf, ist Backup und Restore (Wiederherstellung) bzw. Disaster-Recovery. Man sollte auf jeden Fall Backups durchführen und die Wiederherstellung dieser erproben, damit man bei einem Zwischenfall eine funktionsfähige Lösung mit möglichst geringer Ausfallzeit besitzt und nicht erst dann erproben muss, ob die eigene Lösung funktioniert.

Man kann einen Rechner oft nicht ganz sicher machen, da Fehler in der Software des Betriebssystems oder der eingesetzten Anwendungen möglich sind. Deshalb baut man meist noch ein sicheres Netzwerk um sie herum, oft als „*Perimeter Network*" bezeichnet, das meist aus einer Firewall besteht und somit einen *single point of access* schafft, der nur einen Weg in das Netzwerk bietet.

5.1 Richtiges Verhalten der Benutzer und des Administrators

Dieses Kapitel geht auf die Abhängigkeiten der Computersicherheit von der menschlichen Komponente ein. Dabei ist die Bereitschaft der Benutzer und Administratoren, sichere Maßnahmen zu ergreifen, oft nicht groß genug. Beispielsweise neigen viele Personen dazu, einfache Passwörter zu benutzen, die auch einfach zu erraten sind. Außerdem werden viele Konfigurationsmöglichkeiten in Betriebssystemen nicht genutzt, da sie den Umgang mit diesen komplizierter gestalten. Fehlbedienung durch unwissende Anwender ist ein weiteres großes Problem, das es Angreifern leicht macht, Systeme zu erobern und für ihre Ziele zu missbrauchen. Die Aufklärung von Computerbenutzern sollte mehr Vorrang erlangen, in den Unternehmen und auch allgemein, da die meisten von ihnen noch kein richtiges Sicherheitsbewusstsein ausgebildet haben. Dies mag auch daran liegen, dass viele die dahinterstehenden Techniken nicht verstehen und die Gefahren nicht einschätzen können.

5.1.1 Unsichere Passwörter

Die mit Abstand größte Sicherheitslücke bilden die Passwörter. Einige Benutzer und sogar Administratoren, die Systeme etwa nur zu Testzwecken installieren und dann aus Versehen so belassen, benutzen leere Passwörter, also keine. Auch einfache Passwörter wie Namen von Bekannten, Automarken und Wörter wie „god" oder „test", etc. sind nach Möglichkeit auszuschließen. Die Liste dieser so genannten schwachen (weak) Passwörter ist sehr lang. Es ist einzusehen, dass es für Unternehmen schwierig ist, ihren Mitarbeitern bewusst zu machen, wie wichtig sichere Passwörter sind, gerade weil diese dann nicht mehr einfach zu merken sind und der Benutzer je nach Restriktion auch nicht mehr zwei Passwörter abwechselnd benutzen darf, was unter anderem auch gerne vorkommt.
In einer Security Policy können Passwortkonventionen festgelegt werden, die mit einem System wie Windows 2000 gut durchgesetzt werden können. Dazu müssen die Kennwortrichtlinien im Benutzermanager so definiert werden, dass die Kriterien sicheren Passwörtern entsprechen und das System beim Anlegen oder Ändern eines Passwortes diese dann überprüft und gegebenenfalls das Passwort zurückweisen. Außerdem lässt sich in diesen Richtlinien auch die Arbeits- und somit Anmeldezeit der Mitarbeiter definieren, so dass niemand beispielsweise nachts versuchen könnte, sich als Benutzer anzumelden. Auf diese Weise kann man die Angriffsmöglichkeiten zeitlich auf die Arbeitszeit der Mitarbeiter begrenzen.

Kennwortrichtlinien

Im folgenden werden die allgemein gültigen Richtlinien für Passwörter angegeben. Komplexe Passwörter kann man in Windows 2000 in der Verwaltung unter Lokale Sicherheitsrichtlinie, Kontorichtlinien, Kennwortrichtlinien in dem Punkt „Kennwortrichtlinien müssen den Komplexitätsanforderungen entsprechen" aktivieren, sie sind standardmäßig aber nicht aktiviert.

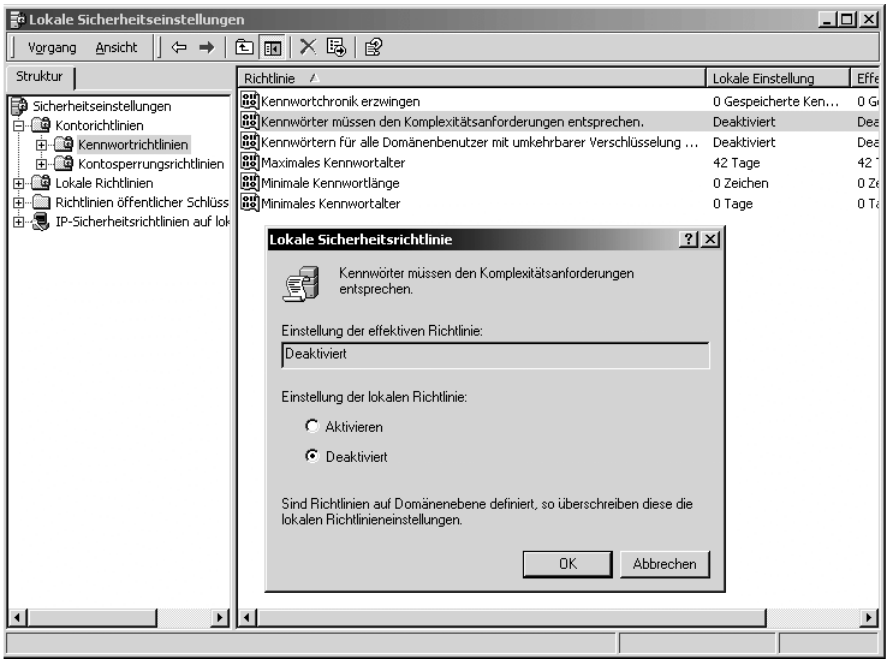

Abbildung 5-1 Lokale Sicherheitseinstellungen - Kennwortrichtlinien

Nach ihrer Aktivierung dürfen Passwörter keinen Benutzernamen und keinen Bestandteil eines vollständigen Namens enthalten und müssen außerdem folgende Kriterien erfüllen:

- mind. 6 Zeichen lang
- Großbuchstaben ohne Umlaute (A,B,C...Z)
- Kleinbuchstaben ohne Umlaute (a,b,c...z)
- Arabische Zahlen (0,1,2...9)
- Nicht-alphanumerische „Metazeichen" (@,#,!,& und so weiter)

Für Windows 2000 sollte zusätzlich in den Benutzerkontenrichtlinien festgelegt werden, dass Passwörter 7 Zeichen lang zu sein haben, die Benutzerkontensperrung nach einer festzulegenden Anzahl von ungültigen Anmeldeversuchen aktiviert wird und es sollte ein Gültigkeitszeitraum für Passwörter festgelegt werden, nach dem ein neues Passwort gewählt werden muss. Der Passwortwechsel sollte vor allem bei Administratorkontos nach höchstens 30 Tagen erfolgen.

Laut [URL08], einem Microsoft Dokument auf der Microsoft Webseite, das unter dem Titel „Ask Us About...Security" abgelegt ist, ist ein sicheres Windows 2000 Passwort 14 Zeichen lang, aber da sich niemand ein so langes Passwort merken kann, wird auch die zweitsicherste Passwortlänge mit 7 Zeichen angegeben. Das liegt daran, dass Passwörter in 7-Zeichen große Blöcke eingeteilt werden, bevor sie in der SAM verschlüsselt gespeichert werden. Beispielsweise ein 10 Zeichen langes Passwort wird in 7 und 3 Zeichen aufgeteilt und die 3 letzten Zeichen sind leicht durch Password Cracker zu erraten. Dies haben wir selbst ausprobiert, man sieht sehr schnell die Zeichen hinter dem ersten Siebenerblock im Klartext und kann dann eventuell schon auf das Wort schließen, anstatt auf die langwierige Entschlüsselung des Wortes zu warten, da der erste Block bei einem 10 Zeichen Passwort viel mehr Aufwand beim Erraten kostet.

Um Passwörter sehr sicher zu machen, kann man nicht-druckbare Zeichen verwenden. Diese sind vor allem gegen das Erraten durch Password Cracking Tools hilfreich. Man kann sie durch das Aktivieren von *Numlock* und anschließendes Drücken der *ALT-Taste* und dem ASCII-Code des Zeichens (z.B. 254) eingeben. Dieses ist für normale Benutzer nicht sehr praktisch, aber für selten benutzte, wichtige Administratoren-Zugänge, z.B. auf Domänen-Controllern, bieten diese Zeichen viel Sicherheit.

Weiterhin gibt es die Möglichkeit mit dem Tool ‚passprop' aus dem Windows 2000 Resource Kit mit dem Befehl: passprop /complex /adminlockout auch das Administratorkonto nach falscher Kennworteingabe zu sperren, da Angreifer meist versuchen werden, dass Passwort des Administrators herauszubekommen. Diese Sperre kann durch den Aufruf von passprop /complex /noadminlockout wieder aufgehoben werden. An der lokalen Konsole kann sich der Administrator allerdings immer wieder anmelden, da ja jemand das System warten können muss. Zusätzliche Sicherheit über die Vorgänge auf dem Rechner bietet die Möglichkeit, in den Überwachungsrichtlinien die Protokollierung misslungener Anmeldeversuche zu aktivieren, um über solche Versuche informiert zu sein.

Aktuelle Sicherheitsprobleme

Eine Sicherheitslücke in der „Protected Store Key Length" ermöglicht es, laut *Microsoft Security Bulletin MS 00-032*, einem lokal angemeldeten Benutzer sicherheits- und kontenrelevante Informationen über andere Benutzer, die diesen Rechner benutzen, herauszufinden. Die Daten eines Benutzers wie der Private Key und Zertifikate werden normalerweise mit der höchsten Verschlüsselungsstufe verschlüsselt, bei der Windows 2000 128-bit Version mit 128 bit, leider werden die Daten fälschlicherweise mit 40 bit-Schlüsseln verschlüsselt. Dies legt die Daten nicht bloß, ihre Verschlüsselung ist aber nicht sehr sicher.

Gegenmaßnahmen

Auf der Microsoft Internetseite ist ein Patch erhältlich, der dieses Problem behebt, er besteht aber aus einer DLL (PSBASE.DLL) und einem Tool (KEYMIGRT.EXE), das von Hand ausgeführt werden muss. Der Patch ist zwar in Service Pack 1 enthalten, das Tool muss jedoch trotzdem ausgeführt werden. Dieser Vorgang ist leider nicht im Service Pack 1 beschrieben und nur schwer zu finden, was man Microsoft negativ anrechnen muss.

5.1.2 Fehlbedienung, Unwissenheit und Ermöglichen von Angriffen

Fehlbedienung, Unwissenheit und Ermöglichen von Angriffen durch Benutzer

Man kann nicht oft genug betonen, dass Firmen selbst dafür verantwortlich sind, ihren Mitarbeitern zu verdeutlichen wie wichtig Sicherheitsmaßnahmen und wie entscheidend ihre Durchführung für das Bewahren eines sicheren Zustands sind. Dabei entfällt ein großer Teil der Verantwortung auf leitende Angestellte, die dafür sorgen müssen, dass ihre Mitarbeiter regelmäßig über Probleme aufgeklärt und ihnen Regeln in geeigneter, übersichtlicher und schnell lesbarer Form zur Verfügung gestellt werden, da sie sonst höchst wahrscheinlich nicht beachtet werden. Es ist wichtig dabei an ihr Verantwortungsbewusstsein zu appellieren und sie in den Prozess zu integrieren.

Generell sollten die Benutzer folgendes wissen:

- Sie sollten über Sicherheit aufgeklärt werden.
- Sie sollten starke Passwörter benutzen, wissen wie sie aufgebaut sind und wieso sie benötigt werden.
- Sie sollten keine fremde Software einführen oder aus dem Internet heruntergeladene einfach ausführen oder installieren.
- Sie sollten keine E-Mail-Attachments mit dubiosen Inhalten oder von unbekannten Adressen öffnen, da dies einer der Hauptgründe für Virenverbreitung ist.
- Sie dürfen nicht einfach sicherheitsrelevante Informationen preisgeben, wenn beispielsweise ein angeblicher Administrator am Telefon nach ihrem Benutzernamen und Passwort fragt.
- Sie sollten die Sicherheitsrichtlinien akzeptieren und nach ihnen handeln.

Fehlbedienung, Unwissenheit und Ermöglichen von Angriffen durch Administratoren

Auch den Administratoren sollte verdeutlicht werden, dass sie normalerweise mit einem Benutzerkonto arbeiten sollten und sich nur im Bedarfsfall über „*runas*", das bei UNIX als su – switch user bekannt ist, die erforderlichen Rechte für den nötigen Zeitraum einräumen können. Dies wird als das „Umschalten zwischen privilegierten und nicht privilegierten Kontexten" bezeichnet und ist unter Windows 2000 mit Hilfe des *sekundären Anmeldedienstes* (SLS – Secondary Logon Service) möglich, aber bei weitem nicht so komfortabel wie unter UNIX. Dabei ergeben sich jedoch zwei Probleme. Der über runas angemeldete Administrator ist immer noch mit seinem Benutzerkonto im System angemeldet und die Meldungen und Prozesse der beiden jetzt angemeldeten Benutzer sind nicht unbedingt zu trennen. Außerdem muss man das System gut kennen, um die richtigen Anwendungen mit runas in der Eingabeaufforderung starten zu können.
Es macht keinen Sinn als Administrator Routinearbeiten zu erledigen, Briefe zu schreiben, im Web zu surfen oder E-Mails zu lesen, dies muss den Administratoren klar sein und sie müssen auch danach handeln und nicht wie sehr oft in der Praxis aus Faulheit als Administrator angemeldet bleiben. Ist man auf seinem Rechner, übrigens auch einem Heimrechner unter Windows 2000 Professional, als Administrator angemeldet und surft im Web, können schon durch Skripte auf Internetseiten verheerende Dinge auf dem Rechner in Gang gesetzt werden, die dann im Kontext des Administratorkontos ablaufen. Der Gebrauch eines normalen Benutzerkontos kann hier den Schaden schon sehr begrenzen.

Ein weiterer unverzeihlicher Fehler, den ein Administrator begehen kann, ist sich mit der Kennung eines Domänenkontos auf einem Stand-Alone-Rechner anzumelden. Dadurch bekommt ein Angreifer Zugriff auf das ganze System, wenn er den Rechner kompromittiert hat. Somit missbraucht er, evtl. unbewusst, seine Vertrauensstellung des Domänenkontos. Das ist eine der größten Sicherheitslücken, die für den Angreifer zum Zugang zu der ganzen Domäne führt. Deshalb sollte man folgende drei Dinge nie tun:

- Lokalen Administratorkonten die gleichen Kennwörter wie Mitgliedern der Gruppe Domänenadministratoren geben
- Lokalen Konten die gleichen Namen und Kennwörter wie Domänenkonten geben, insbesondere bei Mitgliedern der Domänenadministratorengruppe

- Informationen zu Kennwörtern in Kommentarfeldern eingeben, wie etwa: „gleiches Kennwort wie bei Server 2“

Administratoren sollten auch ihre Passwörter nicht für Anmeldungen an beispielsweise FTP-Servern benutzen, da FTP alles, auch die Passwörter, im Klartext überträgt und diese abfangbar sind.

Man sollte auch als Systemadministrator keine Informationen über eingesetzte Hard- und Software preisgeben, die vermeintliche Anbieter von Konkurrenzprodukten haben möchten. Dies ist die gleiche Form von Social Engineering, die in Kapitel 3 genannt wurde, nur auf Administratoren zugeschnitten, von denen man fundiertere Kenntnisse erhalten kann. Das anzuwendende Verhalten ist auch bekannt als „security by obscurity“, der Angreifer kennt die anzugreifenden Ziele nicht, da er keine Informationen herausbekommen kann. Diese sind heutzutage aber nicht mehr so schwer herauszubekommen, also ist dieser Punkt nicht mehr so entscheidend, trotzdem sollte man es potentiellen Angreifern nicht einfacher machen.

Wenn ein Angreifer über Telnet einen administrativen Zugriff hat, kann er, falls ein Administrator vergessen hat sich abzumelden, seine Session übernehmen und somit evtl. wichtige Informationen erlangen. Ein Administrator sollte sich nach einer Telnet-Sitzung immer mit Strg+Alt+Entf abmelden und nicht nur im Client Fenster auf Verbindung beenden klicken.

Man sollte seine Administratorkonten sehr gut schützen, da man mit ‚lsadump2‘, einem Tool von Todd Sabin, den oder die letzten Anmeldevorgänge von Diensten mit ihren Namen und Passwörtern aus der Local Security Authority (LSA) auslesen kann. Unter Windows NT 4.0 ist dies als LSA Secrets bekannt, hier werden die letzten Anmeldungen auf externen Systemen mit Namen, Kennwörtern und Hash-Sequenzen gespeichert und nur ganz leicht verschlüsselt, nachdem sie in Windows NT 4.0 gar nicht verschlüsselt waren. Es gibt keine Gegenmaßnahmen, da Microsoft dies wohl nicht für gefährlich hält und man lsadump2 nur mit SeDebug-Berechtigung ausführen darf, man diese normalerweise aber nur als Administrator hat. Es ist sehr entscheidend auf die Sicherheit seiner Administratorkonten achten.

Empfehlungen

Ein großes Problem für Umsteiger von Windows NT 4.0 ergibt sich durch die neuen Möglichkeiten des Multimaster-Konzepts für Domänencontroller, mit der ein Active Directory zwischen den Domänen repliziert wird, da dieses ein komplettes Umdenken und eine Umstrukturierung der Ressourcen nach sich zieht.

Außerdem sollte man von der Aufgabendelegierung an andere Administratoren gebrauch machen, daher muss die Zugriffsteuerung sehr gezielt für alle Benutzer eingestellt und evtl. Benutzer von anderen Domänen als nicht vertrauenswürdig eingestuft werden. Beispielsweise Partner oder Internet-angebundene Abteilungen sollten eigene Strukturen oder sogar Server bekommen. Durch die größere Gruppe von Administratoren und der domänenglobalen Gruppen, ist die Möglichkeit eines kompromittierenden Kontos in diesen Reihen größer als vorher und sollte deshalb bei der Planung bedacht werden.

Man sollte auch vorsichtig mit der Installation von Tools sein, die man manchmal für Administrativ- oder Testzwecke benötigt, die ein eingedrungener Angreifer jedoch auch gegen einen selbst verwenden könnte, wie z.B. das ‚W2RK' (Windows 2000 Resource Kit) oder Tools aus dem Verzeichnis \Support\Tools der Windows 2000 Server CD. Diese Tools sind natürlich für das Überprüfen der Sicherheitseinstellungen unerlässlich, sollten aber auf Wechseldatenträgern untergebracht werden, um sie vor ungewollter Benutzung zu verbergen.

Wichtig ist auch, niemals bei einem Konto das *automatische Anmelden* in der Systemsteuerung unter Benutzer zu aktivieren, da dann jemand einfach nur den Rechner neu zu starten oder einzuschalten braucht, um Zugriff zu erlangen.

Es sollte nur eine gerade nötige Anzahl Systemadministratoren geben und das Prinzip der verteilten Pflichten durchgesetzt werden. Die Administration bestimmter Teilbereiche sollte niemals von einer Person allein geschehen, sondern nach dem „4-Augen-Prinzip" verteilt werden.

Auf sicheren Systemen wie Firewalls, etc. sollte man sehr vorsichtig mit der Installation von zusätzlicher Software sein, da man meistens nicht weiß, ob diese die Sicherheit eventuell untergräbt.

5.1.3 Aktualisierungen und Updates von Windows 2000

Microsoft bringt nach dem Bekanntwerden von Sicherheitsproblemen so genannte „Hotfixes" heraus, die Patches sind und teilweise in einer bestimmten Reihenfolge ausgeführt werden müssen. Ungefähr halbjährlich fasst Microsoft diese zu so genannten Service Packs zusammen. Ein neuer Service Pack enthält immer die vorherigen, so dass man nur den neuesten installieren muss. Innerhalb dieser Zeiträume sollte man darauf achten, die aktuell erscheinenden Hotfixes zu installieren. Service Packs müssen auch nach der Installation von Software oder Betriebssystemkomponenten noch einmal installiert werden, um auf dem neuesten Stand zu bleiben, da es möglich ist, dass bereits erneuerte Komponenten bei der Installation durch veraltete Versionen ersetzt wurden. Es ist ratsam ein komplett identisches System zu besitzen, um auf diesem Software und Service Packs installieren und deren einwandfreies Funktionieren mit der eigenen Konfiguration testen zu können. Außerdem hat man so, im Falle eines Hardwaredefekts oder Angriffs, sofort einen lauffähigen Ersatzrechner zur Verfügung , vorausgesetzt man kopiert die Daten immer auf den zweiten Rechner. Außerdem hat man dadurch ein zusätzliches Backup.

Bei Windows 2000 hat man die Möglichkeit die Service Packs auf das Installationsverzeichnis der jeweiligen Produkt CD anzuwenden und von dieser aktualisierten Version dann neue Rechner zu installieren. Damit ergibt sich eine erhebliche Vereinfachung im Gegensatz zu Windows NT 4.0, bei dem man in jedem Fall die Service Packs bei einer Neuinstallation anwenden musste. Die einfachste Methode um das aktuelle Service Pack und die wichtigsten Hotfixes auf dem Rechner zu installieren, ist das integrierte *Windows Update*, das nur funktioniert, wenn der Rechner einen Zugang zum Internet und den Microsoft-Internetseiten hat. Dort kann man bequem auf einer Weboberfläche die verfügbaren Updates auswählen und installieren lassen. Leider müssen Hotfixes, die nach Service Pack 2 herausgebracht wurden, immer noch von Hand installiert werden. Es ist wichtig zu wissen, dass Windows Update nur wenige der verfügbaren Hotfixes installiert und

man deswegen immer auf den Microsoft Update Internetseiten nachsehen muss, welche Hotfixes für einen relevant sind und diese dann herunterladen und installieren muss. Dies geschieht nicht automatisch, wie Windows Update es eigentlich propagiert. Bei einem Server im Netzwerk ohne Internet-Anschluß muss man das Service Pack und die Hotfixes auf einem anderen, mit dem Internet verbundenen Rechner, als Dateien speichern und über einen Datenträger auf dem zu aktualisierenden Rechner manuell installieren.

Mit Hilfe der Anwendung ‚qfecheck.exe', die man bei Microsoft auf den Internetseiten herunterladen kann, ist es möglich, sich die bereits installierten Hotfixes anzeigen zu lassen. Außerdem ist das Tool in der Lage, über die Windows File Protection, die installierten Dateien auf ihre Versionen und Intaktheit zu überprüfen. Somit kann man den Stand seiner Installation leicht überprüfen und sehen, ob, durch eventuelle Installationen, wichtige Dateien wieder durch alte Versionen ersetzt wurden.

Zur komfortablen Installation mehrerer Hotfixes auf einmal und ohne lästige Neustarts, bietet sich die Verwendung einer Batchdatei an. Dies wird in einem Artikel auf den Microsoft-Internetseiten vorgeschlagen und erklärt. Nötig hierzu ist allerdings die Option der Hotfixes im stillen Modus abzulaufen und keinen Neustart zu machen. Außerdem muss man sich bei dieser Methode unbedingt an die richtige Reihenfolge der Hotfixes halten. Die Anwendung ‚qchain.exe', die man ebenfalls auf dieser Seite findet, braucht man, um die Installation abschließen zu können.

Ein gerade erst veröffentlichtes Tool, der ‚Microsoft Network Security Hotfix Checker' [URL17], ermöglicht die kommandozeilenorientierte Überprüfung von Computern auf das Vorhandensein oder Fehlen von Patches. Dies funktioniert auch im Netzwerk, kann auf den Microsoft Webseiten heruntergeladen werden und heißt ‚hfnetchk.exe'.

Es gibt einen Bug in Windows 2000, der es laut *Microsoft Security Bulletin MS01-00* ermöglicht, dass installierte Hotfixes deinstalliert werden. Dieser betrifft nur englischsprachige Hotfixes, die älter sind als der vom 18.12.2000. Alle Hotfixes seit dem 19.12.2000 haben dieses Problem nicht mehr. Außerdem müsste laut Microsoft der Administrator die Hotfixes in einer anderen Reihenfolge als ihrem Erscheinen installiert haben, um die Konstellation für den Fehler zu schaffen. Der Fehler beruht darin, dass das Windows File Protection System dazu gebracht werden kann, Dateien, die durch Hotfixes ersetzt wurden, wieder durch die alten fehlerhaften Dateien zu ersetzen. Sämtliche Hotfixes werden in einem Katalog-File gelistet und digital signiert, um ihre Integrität verifizieren zu können und durch WFP überprüfbar zu sein. Bei den betroffenen Hotfixes gab es ein Problem mit dem Katalog-File und deshalb ist die nachträgliche Deinstallation möglich. Alle Service Packs ab Version 1 haben dieses Problem nicht.

5.2 Administrative Einstellungen in Windows 2000

Windows 2000 enthält fast doppelt so viele Dienste wie Windows NT 4.0, dadurch wird das System unübersichtlicher, sie sind jedoch alle in der Microsoft Management Console (MMC) für Dienste aufgeführt.
Neu hinzugekommen sind Gruppen- und Sicherheitsrichtlinien, die über ein grafisches Verwaltungsprogramm konfiguriert werden und viele Richtlinien für die Systemsicherheit festlegen können. Diese Richtlinien verwenden eine hierarchische Vererbungsstruktur und werden ebenfalls im Active Directory gespeichert. Sicherheitsvorlagen definieren viele Einstellungen für diese Richtlinien und können dazu verwendet werden, vorhandene Sicherheitsrichtlinien zu überprüfen oder einzurichten. Diese Vorlagen können sowohl innerhalb einer Domänenstruktur, als auch zwischen zwei fremden Servern ausgetauscht und immer wieder verwendet werden.
In Windows 2000 werden für Objekte DACLs (Discretionary Access Control Lists) benutzt, d.h. dass für jedes Objekt einzeln bestimmt und beim Zugriff überprüft wird, ob und welche Zugriffsrechte der anfordernde Prozess bzw. Benutzer hat und benötigt. Das NTFS, das Active Directory und auch die Registrierung können durch DACLs gesichert werden. Für NTFS gibt es dabei folgende Rechte:

Zugriffsrecht	Beschreibung
R (Read)	Das Objekt kann durch die angegebenen Benutzer oder Gruppen gelesen werden.
W (Write)	Das Objekt kann verändert oder geschrieben werden.
X (Execute)	Einige Objekttypen können ausgeführt werden (z.B. Programme). Wer das Recht zur Ausführung besitzt, wird mit diesem Attribut festgelegt.
D (Delete)	Objekte können gelöscht werden, wenn die Benutzer oder Gruppen dieses Recht besitzen.
P (Change Permission)	Der Benutzer oder die Gruppe darf die Liste der Zugriffsrechte verändern.
O (Take Ownership)	Der Benutzer hat die Möglichkeit, den Besitz zu übernehmen und erlangt dadurch evtl. weitere Rechte an dem Objekt.

Tabelle 5-1 NTFS-Zugriffsrechte

Da die Registrierung eine andere Aufgabe als ein Dateisystem hat und viele sicherheitsrelevante Informationen enthält, sind die Zugriffsrechte für Einträge in der Registrierung um einige Funktionen erweitert. Diese können mit der Anwendung 'regedt32.exe' geändert werden.

Zugriffsrecht	Beschreibung
Q (Query Value)	Der Wert darf gelesen werden.
S (Set Value)	Der Wert darf verändert werden.
C (Create Subkey)	Unterschlüssel können erstellt werden.
E (Enumerate Subkeys)	Die Unterschlüssel können gesehen werden.
N (Notify)	Wird ein Schlüssel oder Wert geändert, wird der Benutzer benachrichtigt.
L (Create Link)	Erlaubt die Erstellung eines symbolischen Links von einem Schlüssel.
D (Delete Key or Value)	Der Schlüssel oder Wert darf gelöscht werden.
P (Write DAC)	Der angegebene Benutzer oder die Gruppe darf die Zugriffsrechte für den Schlüssel oder den Wert ändern.
O (Write Owner)	Der angegebene Benutzer darf den Besitz für den Schlüssel übernehmen.
R (Read Control)	Die Zugriffsrechte dürfen gelesen werden.

Tabelle 5-2 Registrierungszugriffsrechte

Die Installation einer reinen Windows 2000 Umgebung ist einer gemischten Umgebung vorzuziehen, da in der gemischten Umgebung durch Kompatibilität zu alten Anmeldeverfahren und weiteren Komponenten die Sicherheit stark vermindert wird.

Grundlegende Einstellungen

Es gibt einige Einstellungen, die notwendig sind, um die Konfiguration sicherer zu machen. Diese Einstellungen sind natürlich vom Anwendungszweck des Servers oder Computers abhängig und können nicht pauschal angegeben werden.

Benutzerkonten

Nicht benötigte Benutzerkonten können und sollten gelöscht werden, da dies mögliche Angriffe auf Benutzerkonten minimiert. Eine sinnvolle Maßnahme ist auch die Umbenennung des Anmeldenamens des Administratorkontos. Allerdings hat der Administrator immer die RID 500, und ein Angreifer kann über die RID den Administratornamen herausbekommen. Wenn allerdings auf einem sicheren Server RID-Scanning nicht erlaubt ist, wird es schwierig sich als Administrator einzuloggen, da man den Namen, zu dem er umbenannt wurde, nicht so leicht herausbekommt.

BIOS-Einstellungen

Weiterhin sollte man zum lokalen Schutz des Systems BIOS-Passwörter einsetzen und bootfähige Wechsellaufwerke, wie Diskettenlaufwerke, deaktivieren. Außerdem kann man durch BIOS-Passwörter verhindern, dass ein Angreifer den Rechner nach Installation seiner Tools neu starten kann, ohne dass es bemerkt wird. Durch einen Neustart des Computers können von einem Angreifer auf das System übertragene Tools effektiv gestartet und als unsichtbarer Prozess installiert werden.

Registrierung

Die Registrierung kann durch Tools ausgelesen werden, was sehr detaillierte Informationen über die installierte Software, Benutzer und weiteres preisgibt. Sind in der Registrierung die Schlüssel HKLM\SYSTEM\CurrentControlSet\SecurePipeServers\winreg und die untergeordneten Schlüssel vorhanden, ist der Zugriff nur Administratoren erlaubt. Man kann dies durch Patches von Microsoft nachträglich einrichten.

Programme des Administrators

Wichtige Anwendungen, die für die Administration des Systems verwendet werden, sollte man in einem eigenen Ordner unterbringen, dessen Name nicht sofort auf die enthaltenen Programme schließen lässt, und eine Gruppe mit einem genau so unauffälligen Namen anlegen. Die Benutzer dieser Gruppe bekommen dann alleinigen Zugriff auf den Ordner und man kann den Administrator als Mitglied der Gruppe definieren. Außerdem sollte man die Zugriffsrechte der für die Administration verwendeten und im System32-Verzeichnis gespeicherten Anwendungen ändern, damit sie nur durch den Administrator ausgeführt werden können.

Sicherung der SAM

Verwendet ein Windows 2000 Computer kein Active Directory, werden die Benutzerkonten und Passwörter in der *SAM-Datenbank* (System Accounts Manager) gespeichert. Diese ist mit Syskey verschlüsselt und der Schlüssel wird lokal gespeichert. Zur Erhöhung der Sicherheit kann der Schlüssel aber auch auf einer Diskette auslagert werden, diese ist dann allerdings zum Starten des Rechners erforderlich.
Wird Active Directory auf einem Server eingesetzt, werden die Passwörter dort gespeichert. Trotzdem können die Passwörter auch dann verändert werden, dafür muss sich der Angreifer direkt am Server befinden und diesen neustarten können.

NetBIOS und Null-Sessions

NetBIOS ermöglicht in Windows NT 4.0 die Anmeldung eines anonymen Benutzers durch so genannte Null-Sessions. Dies ist auch noch unter Windows 2000 möglich und kann von einem Angreifer dazu verwendet werden, um Benutzerinformationen und Registrierungseinträge über das Netzwerk auszulesen.
Um diese Sicherheitslücke zu schließen, muss die Option NetBIOS über TCP/IP deaktivieren in den WINS-Netzwerkeinstellungen für das TCP/IP-Protokoll der Netzwerkkarte ausgewählt werden, wodurch auch die Ports 135 und 139 deaktiviert werden.
Damit Null-Sessions nicht mehr funktionieren, muss allerdings auch der Wert *RestrictAnonymous* in der Registrierung (HKLM\SYSTEM\CurrentControlSet\Control\Lsa) auf 1 gesetzt werden.
Wird nur NetBIOS über TCP/IP deaktiviert, sind Null-Session weiterhin möglich, allerdings für einen Angreifer nur eingeschränkt nutzbar.

Lokale Anmeldung

Bei einem Server sollte generell in den lokalen Richtlinien unter den Benutzerrechten darauf geachtet werden, wer sich lokal anmelden darf. Benutzer, speziell der Benutzer Gast, sollten sich auf gar keinen Fall lokal anmelden dürfen, da es sich um keinen Arbeitsplatzrechner handelt und es Angreifern leichter gemacht wird, wenn sie mehr Konten als nur das Administratorkonto für ihre Angriffe zur Verfügung haben.

Administration aus der Ferne

Soll ein System sicher aus der Ferne verwaltet werde, bietet Windows 2000 die Terminaldienste, die im Kapitel 2.2.8 und 4.2.7 behandelt werden. Außerdem gibt es eine Reihe von Anwendungen von Drittherstellern, die diese Funktionen ebenfalls bieten.

5.2.1 Einschränken und Entfernen von Diensten und Komponenten

Die Entscheidung, welche Dienste und Anwendungen auf einem Rechner, beispielsweise einem Server, benötigt werden, hängen sehr stark von seinem Einsatzgebiet ab. Dieser Punkt ist sehr entscheidend für die Sicherheit des Systems. Je weniger Dienste auf einem angriffsgefährdeten Server ausgeführt werden, desto besser, da man damit seine Angreifbarkeit herabsetzt. Jede zusätzliche Software auf einem System, die man nicht verwendet, könnte von einem Angreifer als Versteck für einen Trojaner benutzt werden. Deshalb ist das Löschen von nicht benötigten Komponenten sehr wichtig, und derer gibt es viele bei normalen Windows 2000 Installationen. Man sollte auf jeden Fall auf installierte Programme wie z.B. ‚Rechner' oder ‚Imaging', die man nicht verwendet, verzichten und sie löschen. Generell gilt es auch, nur soviel Software von anderen Anbietern zu installieren, wie unbedingt notwendig ist und diese vorher nach Möglichkeit zu testen. Weitere eventuell überflüssige Komponenten sind ‚HyperTerminal', die ‚Wählhilfe', installierte Modems, Spiele, der ‚CD-Spieler' und andere Unterhaltungsmedienprogramme, die auf einem produktiven Rechner evtl. nicht benötigt werden.

Die Windows 2000 Server-Version enthält noch weitere Komponenten, bei denen man die Notwendigkeit kritisch prüfen sollte. Hierzu gehören:

- Zubehör und Dienstprogramme, z.B. der erwähnte CD-Spieler und Rechner, die selten benötigt werden.
- Indexdienst – Erstellt Indizes von allen möglichen Daten. Die Verwendung des Indexdienstes ist nicht unbedingt erforderlich, erhöht aber die Geschwindigkeit von Volltextsuchen. Da dieser Dienst allerdings einige Sicherheitslücken aufweist und in der Vergangenheit oft Ziel von Angriffen war, sollte die Aktivierung gut überlegt werden.
- Internet Information Server (IIS) – Selbst wenn kein Webserver benötigt wird, kann es erforderlich sein, diesen Dienst zu installieren, da dieser folgende Serverdienste zur Verfügung stellt, die von anderen Programmen evtl. benötigt werden: FTP-, SMTP-, NNTP-, IPP- und WebDAV-Server.
- Verwaltungs- und Überwachungswerkzeuge – Einige können hilfreich sein, helfen aber auch Angreifern bei ihren Zielen.

- Message Queuing Dienste – Bieten eine Kommunikationsinfrastruktur und werden zur Verteilung von Nachrichten zwischen Anwendungen und Verwaltung von Warteschlangen verwendet.
- Netzwerkdienste – Die Verwendung der Netzwerkdienste sollte genau überlegt werden, da hierüber viele Angriffe möglich sind und getätigte Einstellungen die Systemsicherheit extrem beeinflussen.
- Remoteinstallationsdienste – Wenn es nicht geplant ist, Rechner vom Netzwerk aus zu installieren, wird diese Komponente nicht benötigt.
- Remotespeicher – Hiermit kann man Daten bei großen zu verarbeitenden Datenmengen auf langsamen Medien (z.B. Bändern) auslagern. Dieser Dienst wird auch von dem in Windows integrierten Backup-Programm verwendet.
- Script Debugger – Ist für Entwicklungssysteme sinnvoll, aber nicht für Server.
- Terminaldienste und -lizenzierung – Wenn man keine Clients als Terminals nutzen will, sollte man diese Komponente unbedingt löschen, da sie in letzter Zeit auch das Ziel von Angriffen war. Außerdem wird schon durch das Vorhandensein der Terminaldienste eine entfernte Anmeldung von Benutzergruppen möglich, die sonst nicht angeboten wird.
- Windows Media Dienste – Wenn der Server nicht zu Streaming-Zwecken eingesetzt werden soll, wird diese Komponente nicht benötigt.

Generell sollte man mögliche Sicherheitsprobleme, die durch das Ausführen oder Vorhandensein von nicht benötigten Diensten bestehen, ganz einfach dadurch verhindern, dass man diese entfernt oder komplett deaktiviert.
Mit Hilfe des Diensteverwaltungsprogramms ‚*services.msc*' kann man sich die laufenden Dienste anschauen, starten, beenden und deaktivieren, das Programm befindet sich auch unter Verwaltung, Dienste. Speziell für die Anzeige der TCP/IP-Netzwerkverbindungen eignet sich das Tool ‚*netstat*' das mit dem Aufruf ‚netstat -an' alle aktiven Netzwerkverbindungen anzeigt. Anhand der Liste kann man entscheiden, welche Netzwerkdienste man nicht benötigt und diese dann deaktivieren, was die Sicherheit erhöht.
Die Entfernung der Systemzubehörkomponenten ist auf einem Windows 2000 Client nicht einfach möglich, da diese nicht in den Windowskomponenten in der Software-Systemsteuerung vorhanden sind. Dazu muss die Datei ‚sysoc.inf' im Verzeichnis Winnt\inf bearbeitet werden.
Der Punkt Zubehör und Dienstprogramme erscheint in den Windowskomponenten, wenn das Wort ‚HIDE' im Eintrag ‚Games=ocgen.dll,OcEntry,games.inf,HIDE,7' in der Datei entfernt wird [URL21]. Die Serverversion von Windows 2000 benötigt diese Änderung an der Datei nicht, da die Komponenten angezeigt werden.

Weitere wichtige Dienste

Es sollte auf jeden Fall der SNMP-Agent entfernt oder der SNMP-Dienst ausgeschaltet werden, wird es allerdings intern verwendet, müssen auf jeden Fall Port 161 und 162 in einer Firewall abgeschirmt werden, da SNMP-Dienste sonst von einem öffentlichen Netzwerk aus erreicht werden könnten. Eine weitere Möglichkeit besteht darin, die SNMP Berechtigungen von public auf private zu ändern, damit kein anonymer Zugriff möglich ist.

5.2.2 Verwendung von Richtlinien und Sicherheitsvorlagen

Windows 2000 verwaltet viele *Sicherheitseinstellungen* in so genannten *Richtlinien*. Diese werden zentral auf einem Server oder auf einem lokalen Computer eingerichtet und betreffen z.B. Passwortrichtlinien oder bestimmen, wer sich lokal an einem Server anmelden darf.
Mit Hilfe dieser Richtlinien ist es einem Administrator möglich, diverse Einstellungen für diese Richtlinien an einem Domänencontroller vorzunehmen, die Einstellungen werden dann an die Windows 2000 Clients übertragen und angewandt.

Richtlinienvererbung

Die Richtlinien in einer Domänenstruktur werden im Active Directory gespeichert und haben Auswirkungen auf alle Windows 2000 Clients und Server, die der Domäne angehören.
Die Verwaltung dieser Richtlinien erfolgt in vier Ebenen:

- **Richtlinien für Organisationseinheiten (OUs)**
  Computer können in Organisationseinheiten zusammengefasst werden. Einstellungen an den Richtlinien für OUs werden auf allen Windows 2000 Computern durchgesetzt, die dieser OU angehören. Jede Windows 2000 Domäne enthält eine OU, die die Domänencontroller der Domäne zusammenfasst. Die Sicherheitseinstellungen für Domänencontroller sind solche Richtlinien einer OU.
- **Richtlinien für Domänen**
  Für jede Domäne oder Unterdomäne können Richtlinien definiert werden. Diese werden nur durch Richtlinien aus Organisationseinheiten überschrieben. Jede Windows 2000 Domäne enthält eine solche Richtlinie.
- **Standortrichtlinien**
  Computer gehören zu einem Standort, der im Active Directory definiert wird. Auch für einen Standort können Richtlinien definiert werden, die von den Domänen- und OU-Richtlinien überschrieben werden können.
- **Lokale Richtlinien**
  Die unterste Ebene bilden die lokalen Richtlinien, die direkt auf einem Computer definiert werden. Sie bestimmen die Richtlinien, die von keinen Richtlinien aus den anderen Ebenen definiert werden. Lokale Richtlinien können auch ohne eine Windows 2000 Domänenstruktur und ohne das Active Directory erstellt werden.

Richtlinien können nun in jeder Ebene definiert werden. Wird eine Richtlinie schon in einer Richtlinie mit höherer Priorität festgelegt, überschreibt diese ihre Einstellungen. Werden einzelne Richtlinien nicht definiert, so werden Richtlinien mit geringerer Priorität verwendet.

Richtlinienreplikation und -anwendung

Alle nicht lokalen Richtlinien werden im Active Directory gespeichert und über die Domäne repliziert. Wird ein Computer neu gestartet, wird er im Active Directory nach Richtlinien suchen, die ihn betreffen. Richtlinien können sowohl Computereinstellungen betreffen, diese werden eingerichtet, wenn ein Computer gestartet wird, als auch Benutzereinstellungen definieren, die erst dann übernommen werden, wenn sich ein Benutzer am System anmeldet.

Zusätzlich zur Übertragung der Richtlinien beim Starten eines Computers oder Anmelden eines Benutzer werden diese in regelmäßigen Abständen repliziert. Die Zeitdauer zwischen den Aktualisierungen kann ebenfalls durch eine Richtlinie festgelegt werden und ist abhängig davon, ob es sich um eine Replikation zwischen zwei Standorten oder innerhalb eines Standortes handelt.
Soll ein Richtlinienänderung sofort an andere Computer übertragen werden, kann dies mit dem ‚secedit' Befehl geschehen. Das ‚secedit'-Programm kann auch zur konsolenbasierten Einrichtung und Änderung von Richtlinien verwendet werden. Der Befehl ‚secedit /refreshpolicy machine_policy' bzw. ‚secedit /refreshpolicy user_policy' sorgt dafür, dass die entsprechenden Richtlinien sofort übertragen werden.

Konfiguration von Sicherheitsrichtlinien

Sicherheitsrichtlinien sind ein Bestandteil der Gruppenrichtlinien und beinhalten Einstellungen, die für die Sicherheit des Systems oder der Domäne relevant sind. Die Sicherheitsrichtlinien können direkt in der Computerverwaltung verändert werden, notwendige Verwaltungsprogramme sind bereits eingerichtet. Das Programm „Lokale Sicherheitseinstellungen" konfiguriert die lokalen Sicherheitsrichtlinien, deren Einstellungen aber unter Umständen von Richtlinien, die für einen Standort, eine Domäne oder eine Organisationseinheit definiert sind, überschrieben werden.
Ist der verwendete Server ein Domänencontroller, sind noch die Verwaltungsprogramme für die Domänensicherheitseinstellungen und für die Sicherheitseinstellungen der OU „Domänencontroller" vorhanden.
Die konfigurierbaren Richtlinien sind in folgende Gruppen aufgeteilt:

- **Kontorichtlinien**
  Legen die Sicherheitseinstellungen der Benutzerkonten fest.
- **Kennwortrichtlinien**
  Legen die Sicherheitseinstellungen für Kennwörter fest. Minimale Länge eines Kennworts und die Verwendung von *Kennwortchroniken* werden dort eingestellt.
- **Kontosperrungsrichtlinien**
  Legen unter anderem fest, welche Aktionen dazu führen, dass ein Benutzerkonto gesperrt wird.
- **Kerberos Richtlinien**
  Verschiedene Einstellungen für das Kerberos-System, wie z.B. die Gültigkeitsdauer von Tickets.
- **Überwachungsrichtlinien**
  Sollen Objekte, Dateien oder Benutzer überwacht werden, muss an dieser Stelle die Überwachung aktiviert werden. Es können unterschiedliche Aktionen auf Fehler oder Erfolge überwacht werden.
- **Benutzerrechte und Sicherheitsoptionen**
  Bestimmte Benutzer oder Konten können weitere Sicherheitseinstellungen oder Zugriffsrechte erhalten. Welcher Benutzer sich lokal oder über das Netzwerk an einem Computer anmelden darf, wird z.B. in diesen Richtlinien definiert.
- **Richtlinien öffentlicher Schlüssel**
  Richtlinien für Zertifikate und öffentliche Schlüssel

- **IP-Sicherheitsrichtlinien**
  Richtlinien zu IP-Sicherheitseinstellungen, z.B. zu IPSec.
- **Ereignisprotokollrichtlinien**
  Legen fest, welche Aktionen z.B. durchgeführt werden, wenn ein Ereignisprotokoll voll ist und wie lange Protokolleinträge aufbewahrt werden.

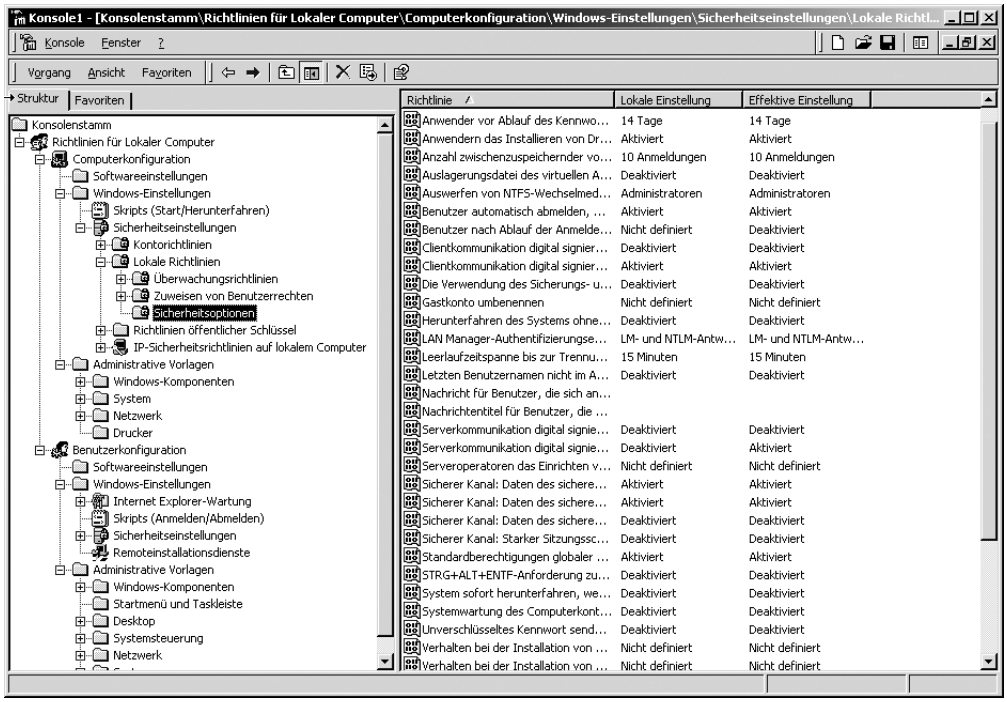

Abbildung 5-2 Konfiguration der wichtigsten Sicherheitsrichtlinien

Konfiguration von Gruppenrichtlinien

Die *Sicherheitsrichtlinien* sind Teil der *Gruppenrichtlinien*, die weitere Einstellungen definieren. Sie sind in Benutzereinstellungen und Computereinstellungen unterteilt und werden entweder mit dem Befehl ‚gpedit.msc', mit dem die lokalen Gruppenrichtlinien konfiguriert werden können, oder über das Active Directory eingerichtet. Dazu wählt man eine Domäne, einen Standort oder eine Organisationseinheit und öffnet die Eigenschaften des Objekts. Dort können Gruppenrichtlinien geändert und neu hinzugefügt werden.
Die Benutzereinstellungen werden angewendet, wenn sich ein Benutzer an einem Computer anmeldet. Die Computereinstellungen werden bei einem Neustart angewendet und aus dem Netzwerk bezogen. Beide Einstellungen werden ebenfalls in regelmäßigen Abständen auf alle Computer der Domäne übertragen.
Die Computereinstellungen der Gruppenrichtlinien enthalten folgende Unterpunkte:

- **Windows Komponenten**
  Diese Richtlinien enthalten Einstellungen für verwendete Programmen. Es können die Programme ‚NetMeeting', ‚Internet Explorer', ‚Taskplaner' und der ‚Windows Installer' konfiguriert werden.

- **System**
  Enthält Einstellungen, die das System betreffen. Dazu gehören Einstellungen zur Anmeldung, Datenträgerkontingente, DNS-Clients, Updatezyklen der Gruppenrichtlinien und der Windows Dateischutz.
- **Netzwerk**
  Einstellungen für Offlinedateien, das Netzwerk und DFÜ-Einstellungen
- **Drucker**
  Einstellungen zu Druckerwarteschlangen, Druckerveröffentlichungen usw.

Die Gruppenrichtlinien enthalten außerdem Einstellungen, die Benutzer betreffen. Diese enthalten Konfigurationen für verwendete Software, Orderumleitungen für Benutzer und Remoteinstallationsdienste, mit denen Software auf Clients installiert werden kann.

Sicherheitsvorlagen

Ein weiteres Tool zur Verwaltung von Sicherheitsrichtlinien sind die Sicherheitsvorlagen. Wie der Name vermuten lässt, handelt es sich dabei um eine Vorlage, die Sicherheitseinstellungen enthält. Diese Vorlage kann dazu verwendet werden, die Sicherheitsrichtlinien auf einem System zu überprüfen oder um diese an die Vorlage anzupassen.

Verwaltung von Sicherheitsvorlagen

Die Sicherheitsvorlagen werden ebenfalls über die Microsoft Management Console verwaltet. Dazu wird eine leere MMC geöffnet (Befehl: ‚mmc'), in die dann das Snap-In ‚Sicherheitsvorlagen' geladen wird. Es sind bereits eine Reihe von Sicherheitsvorlagen definiert, die als Ausgangspunkt für eigene Vorlagen verwendet werden können. Sie sollten auf jeden Fall an ein System angepasst werden, da sie nur als Beispiel für eine sinnvolle Vorlage dienen können.

Analyse eines Systems

Für die Analyse eines Systems muss das Snap-In ‚Sicherheitskonfiguration und -Analyse' in die MMC geladen werden. Dann muss zuerst eine neue Datenbank angelegt werden, in die eine Sicherheitsvorlage importiert wird.
Im Menü der MMC kann der Befehl ‚Computer jetzt analysieren' ausgewählt werden. In der Liste der Sicherheitseinstellungen werden Übereinstimmungen mit der Vorlage durch einen grünen Haken und Fehler mit einem roten Kreuz markiert.

Konfiguration eines Systems

Mit dem Snap-In ‚Sicherheitskonfiguration und -Analyse' kann ein System genauso konfiguriert werden. Dazu wird wieder eine Datenbank erstellt und eine Sicherheitsvorlage importiert. Dann wird die Aktion ‚System jetzt konfigurieren' ausgewählt. Die Einstellungen der Sicherheitsvorlage werden nun auf die Sicherheitseinstellungen übertragen. Zur Dokumentation der Veränderungen, wird ein Protokoll angelegt.

5.3 Überwachung

5.3.1 Überwachung des Systems

Windows 2000 bietet aufgrund seiner Systemstruktur umfangreiche Möglichkeiten der Überwachung und Aufzeichnung von Ereignissen.
Windows unterscheidet dabei zwischen verschiedenen Ereignistypen, die das System in verschiedenen Protokollen speichert. Die wichtigsten Protokolle sind in der Ereignisanzeige der Systemverwaltung enthalten und können dort überwacht werden. Dazu sind verschiedene Sortier- und Filterfunktionen vorhanden, allerdings können diese Protokolle sehr schnell viele Einträge enthalten, so dass die integrierten Methoden zur Kontrolle dieser Einträge nicht mehr ausreichen. Dann empfiehlt sich die Anwendung einer zusätzlichen Software, die die Einträge auf bekannte Probleme hin analysiert.
Einige Programme verwenden eigene Protokolldateien, die im Dateisystem angelegt werden. Besucherprotokolle für Web- oder FTP-Verzeichnisse werden vom IIS in Textdateien protokolliert, die bei einem häufig besuchten Server schnell nicht mehr manuell analysiert werden können, um z.B. Angriffe erkennen zu können. Auch andere Programme, wie beispielsweise der Microsoft SQL-Server verwenden eigene Protokolle in Form von Textdateien.

Erkennen von Angriffen

Durch die Überwachung der Protokolldateien lässt sich ein Angriff erkennen. Oft passiert es, das Administratoren in Unternehmen ihre Systeme sicher machen und die Überwachung aktivieren, sich dann aber nach kurzer Zeit die Protokolle nicht mehr anschauen. Darin bergen sich natürlich große Gefahren, da man nicht weiß, ob man Opfer von Angriffen war oder ist und dementsprechend seine Strategie nicht anpassen kann, um seine Sicherheit an die neuen Gegebenheiten anzupassen. Ein laufendes sicheres System muss permanent überwacht werden. Dazu gehört auch das Erstellen von Backups und das Protokoll-Management, unter dem man das regelmäßige, am besten tägliche, Kopieren der Protokolle auf andere Rechner versteht, damit man eine Möglichkeit zum Einsehen der echten Protokolle hat und erkennen kann, ob sie durch einen Angreifer verändert wurden, da diese oft ihre Spuren verwischen.

Analyse von Protokollen

Da die Protokollanalyse mit Hilfe der Ereignisanzeige von Windows 2000 sehr mühsam sein kann, ist es sinnvoll die Daten in eine Datenbank zu exportieren und dort eventuell Analysen zu automatisieren oder spezielle Software einzusetzen, die bei Zwischenfällen auch gleich Alarmmeldungen generieren kann und die Protokollanalyse über das Netzwerk ermöglicht.

Windows Ereignisprotokolle

Windows 2000 kann sehr viele Ereignisse überwachen und es gibt insgesamt sechs Protokolle in der Windows Ereignisanzeige:

- Das *Anwendungsprotokoll:* Hier tragen Anwendungen ihre Ereignisse ein. Softwarehersteller können Programme so programmieren, dass sie sich im Überwachungssystem selbst eintragen und dann Ereignisse ins Protokoll schreiben können.

- Das *Systemprotokoll:* Es enthält Ereignisseinträge vom Windows 2000 System und eingesetzten Treibern.
- Das *Sicherheitsprotokoll:* Hier stehen Einträge zu Überwachungen von Benutzern, Diensten, Komponenten und Objekten. Einträge werden entweder als erfolgreich oder fehlgeschlagen eingetragen und diese Eintragungen darf nur das System vernehmen, deshalb speichern die meisten Anwendungen ihre Informationen in anderen Protokollen.
- Das *Verzeichnisdienstprotokoll:* Es enthält Einträge von Ereignissen, die den Verzeichnisdienst (Active Directory) betreffen. Dazu zählen Informationen über das Defragmentieren der Verzeichnisdatenbank oder Informationen des Meldedienstes.
- Das *Dateireplikationsdienstprotokoll:* Es enthält Informationen über den Start des Replikationsdienstes und erfolgte Replikationen.
- Das *DNS-Server-Protokoll:* Es beinhaltet Einträge über den Start und das Ende des DNS-Dienstes, Fehlermeldungen und Mitteilungen über die DNS-Zonen.

Das Sicherheitsprotokoll

Nur beim Sicherheitsprotokoll kann explizit festlegt werden, was aufgezeichnet werden. In der Überwachungsrichtlinie wird definiert, welche Ereignisse im Sicherheitsprotokoll festgehalten werden. Sie enthält folgende Optionen und kann festlegen, ob erfolgreiche oder erfolglose Aktionen protokolliert werden:

- *Anmeldeversuche überwachen:* Erfolgreiche und fehlerhafte Anmeldeversuche über das Netzwerk am Computer werden hier erfasst.
- *Anmeldeereignisse überwachen:* Diese Option bewirkt das Aufzeichnen des Anmeldevorgangs am lokalen Rechner.
- *Kontenverwaltung überwachen:* Das Erstellen, Löschen und Verändern von Benutzerkonten und -gruppen wird aufgezeichnet.
- *Active Directory-Zugriff überwachen:* Diese Option steht nur auf Windows 2000 Domänenkontrollern zur Verfügung und protokolliert Zugriffe auf das Active Directory.
- *Objektzugriffsversuche überwachen:* Hier wird die Überwachung für den Zugriff auf Dateien, Verzeichnisse und Drucker aktiviert.
- *Richtlinienänderung überwachen:* Diese Option führt zur Überwachung von Änderungen an den Sicherheits- und Gruppenrichtlinien.
- *Rechteverwendung überwachen:* Es wird protokolliert, ob ein Benutzer versucht hat ein Zugriffsrecht zu verwenden.
- *Vorgangsprotokollierung überwachen:* hiermit werden z.B. Vorgangsaktivierung und –beendigung protokolliert.
- *Systemereignisse überwachen:* Es werden erfolgreiche oder fehlgeschlagene Ereignisse überwacht, die die Sicherheit des ganzen Systems beeinträchtigen.

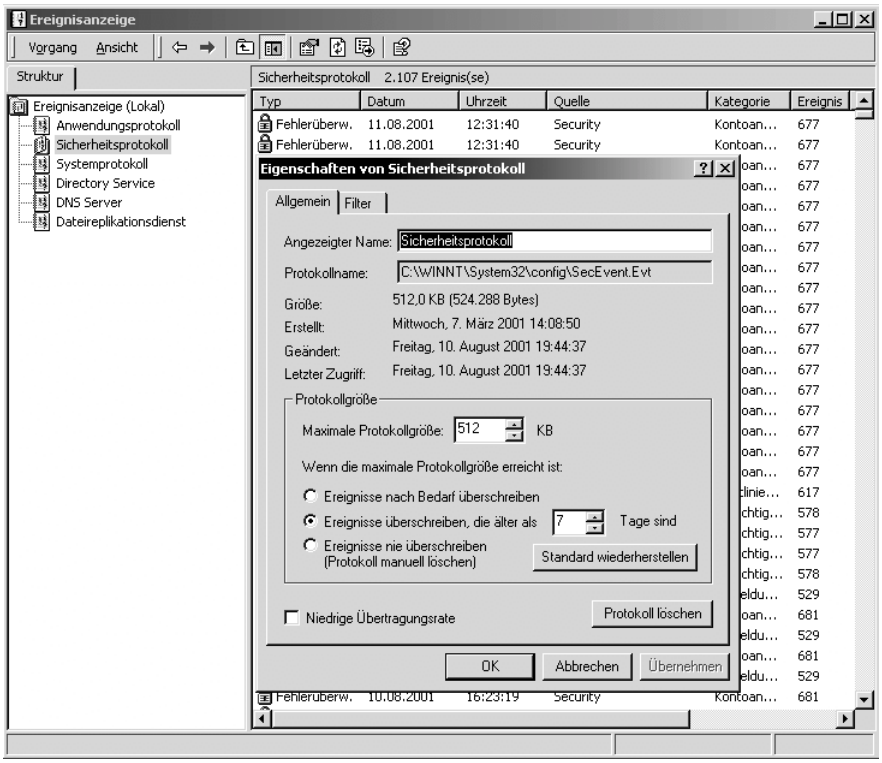

Abbildung 5-3 Ereignisanzeige - Sicherheitsprotokoll

5.3.2 Überwachung der Benutzer

Durch die Einstellungen für das Sicherheitsprotokoll können Zugriffe und Anmeldungen von Benutzern überwacht werden. Wird die Überwachung für Objekte aktiviert, werden allerdings nicht alle Zugriffe aufgezeichnet, sie muss für die betroffenen Objekte aktiviert werden.
Diese Einstellungen werden normalerweise in den Sicherheitseinstellungen der Objekte vorgenommen, wie z.B. bei Dateien und Verzeichnissen. Die Sicherheitsfunktionen von Windows 2000 erlauben es, den Zugriff auf so gut wie alle Objekte zu überwachen, die durch DACLs geschützt sind.
Die Benutzer haben normalerweise keine Möglichkeit, diese Überwachung zu verhindern und Angreifer können nur sehr schwer ihre hinterlassenen Spuren verwischen. Administratoren können durch das Sicherheitsprotokoll nachvollziehen, welche Zugriffe, egal ob erlaubt oder nicht erlaubt, durch Benutzer durchgeführt und evtl. verhindert wurden.

5.3.3 Überwachung der Administratoren

Bei der Überwachung der Administratoren besteht das Hauptproblem in der Tatsache, dass sie Zugriff auf alle Objekte im System haben. Sie sind allmächtig, da sie alle Zugriffsrechte haben, sich vom Benutzer verschlüsselte Dateien anschauen können, Sicherheitseinstellungen ändern und Protokolle löschen können. Sie können großen Schaden anrichten und ihre Spuren effektiv verwischen. Ein Domänenadministrator kann das nur in seiner Domäne, aber ein Administrator des gesamten Netzwerks kann das überall.

Eine persönliche Überwachungsmaßnahme, die nicht unbedingt etwas mit dem Betriebssystem zu tun hat, ist die Überwachung durch das „4-Augen-Prinzip". Hierbei setzt man an administrativer Stelle zwei gleichberechtigte Administratoren ein, die sich gegenseitig überwachen sollen. Dies funktioniert meist sehr gut, es sei denn die beiden verfolgen gleiche Ziele.

Durch die granularere Rechtevergabe ist es jedoch in Windows 2000 auch möglich, weniger Administratoren einsetzen zu müssen als unter Windows NT 4.0. Dadurch ist das ganze System nicht mehr so anfällig für solche Arten von Manipulationen und Angriffen, da man die Anzahl der zu überwachenden Administratoren einschränkt.

Eine weitere nützliche Funktionalität ist die Aufgabendelegierung für administrative Aufgaben. Mit ihr können bestimmte Aufgabenbereiche an eingeschränkte Administratoren verteilt werden, die nur für ihre speziellen Aufgaben, beispielsweise die Benutzerverwaltung, autorisiert sind. Wird von der Aufgabendelegierung intensiv gebraucht gemacht, kann sich der Haupt-Administrator um wichtige Aufgaben kümmern und alltägliche Arbeiten an eingeschränkte Administratoren weitergeben, die mit ihren Rechten nicht sehr viel Unfug treiben können. Ein Problem bleibt hier natürlich immer noch der Haupt-Administrator.

Fazit

Eine funktionierende Überwachung ist nützlich, um Vorkommen und Ausmaß von Zwischenfällen zu protokollieren, sie nachvollziehen und beweisen zu können. Man muss allerdings abwägen, wie detailliert die Überwachung stattfinden soll und welche Ziele sie hat, da zu viele Optionen einen teilweise deutlichen Performanceverlust nach sich ziehen können. Generell bedeutet Überwachung immer einen Leistungsverlust im System, der jedoch auf jeden Fall in Kauf genommen werden sollte.

5.4 Weitere Sicherheitsmaßnahmen

Die Sicherheit von Windows 2000 hängt im Wesentlichen von der Konfiguration des Systems ab. Ein einzelner Windows 2000 Computer kann so abgesichert werden, dass er durchaus direkt mit dem Internet verbunden werden kann.
Ein einzelner Windows 2000 Computer ist aber eher die Ausnahme. Meistens werden einige Server, Arbeitsstationen und Computer mit anderen Betriebssystemen in einem Netzwerk zusammenarbeiten, das von einer zentralen Stelle administriert wird. Wird solch ein Netzwerk größer, kann es vorkommen, dass einzelne Computer nicht ideal konfiguriert sind und dadurch die Sicherheit des gesamten Netzwerks gefährden.
Ein Administrator, der für das Netzwerk verantwortlich ist, wird weitere Sicherheitssysteme verwenden und sich nicht auf eine Sicherheitskomponente verlassen. Ist das Netzwerk an ein öffentliches Netz angeschlossen, empfiehlt sich die Verwendung von Firewalls, Antiviren-Software und IDS-Systemen.

5.4.1 Anti-Viren-Software

Viren, Würmer und andere feindliche oder schädliche Software stellen eine immer größer werdende Gefahr für vernetzte Systeme dar. Die Verwendung von Antiviren-Software soll die Systeme eines Netzwerks vor Viren schützen oder diese aufspüren und zerstören.
Aber auch eine Antiviren-Software muss in einem Sicherheitskonzept verankert sein, damit kein Mitarbeiter ein Virus auf einer Diskette in das Netzwerk einschleusen kann, obwohl der eingehende E-Mail-Verkehr auf Viren überprüft wird.
Es gibt daher unterschiedliche Ansätze, ein System vor Viren zu schützen. Die meisten Systeme verhindern das Einschleusen eines Virus durch Überprüfen von Disketten oder E-Mails. Dabei sind alle Virenscanner dieser Art nur so gut, wie sie aktuell sind. Es sind meistens die aktuellen Viren und Würmer, die Probleme bereiten und ältere Virensoftware wird diese nicht aufhalten.
Daher ist auch eine Antivirensoftware kein Programm, das installiert wird und dann von alleine funktioniert. Es muss sichergestellt sein, dass aktuelle Signaturen von Viren verfügbar sind und auch installiert werden.

Anti-Viren-Software auf einem Server

Werden Antiviren-Programme auf einem Server installiert, müssen diese für solch einen Einsatz optimiert sein. Vielleicht prüft ein Virenscanner nur bei einem Neustart das System auf Virenbefall, ein Server wird aber nur sehr selten neu gestartet und würde daher auch nicht überprüft werden. Es gibt daher eine Reihe von Programmen, die speziell für den Servereinsatz entwickelt worden sind und auch die Administration von Antiviren-Software auf den Clients erleichtern. Spezielle Virenscanner können in vorhandene E-Mail- oder Firewallsysteme integriert werden und scannen ein- und ausgehende Daten auf vorhandene Viren.

5.4.2 Firewalls

In der Regel wird in einer Firewall ein Computer gesehen, der ein internes Netz mit einem unsicheren Netz verbindet und dafür sorgt, dass keine Angriffe auf das interne Netz möglich sind. In der Tat ist das der häufigste Verwendungszweck einer Firewall, aber man muss sich von der Vorstellung trennen, dass eine Firewall ein internes Netzwerk hundertprozentig absichern kann.
Zuerst einmal wird eine Firewall nicht alleine durch die Installation einer Firewall-Software sicher. Vielmehr ist eine Firewall nur ein Werkzeug, um Teile einer Sicherheitspolitik durchsetzen zu können. Für einen wirklichen Schutz sind noch weitere Maßnahmen notwendig. Welchen Sinn macht eine Firewall bspw., wenn der Angreifer sich bereits im Unternehmen befindet oder der Angreifer einen Mitarbeiter einfach bestochen hat?
Die Verbindung des internen Firmennetzes mit einem öffentlichen und unsicheren Netzwerk, wie dem Internet, kann allerdings durch eine gut konfigurierte Firewall insoweit abgesichert werden, als viele Amateure schon einmal ausgesperrt werden.

Installation einer Firewall

Eine Firewall ist kein Produkt, das man kauft, installiert, konfiguriert und dann vergisst. Eine Firewall muss beobachtet und gepflegt werden, Angriffe müssen entdeckt und die Firewall angepasst werden. All dies erfordert Zeit und ein Netzwerkadministrator, der denkt er könnte sich die Arbeit durch eine Firewall erleichtern, sieht das offensichtlich falsch.

Zuerst sollte das richtige Firewall-Produkt gefunden werden, mit dem sich der Administrator entweder auskennt oder jemanden damit beauftragen kann. Es muss geklärt werden, welche Funktionen die Firewall erfüllen muss, ob es noch weitere Einstiegspunkte ins Netzwerk gibt (z.B. eine Einwahlverbindung) und welches Firewall-Konzept das richtige ist.
Generell wird man allerdings feststellen, dass jede Firewall, die nicht völlig falsch konfiguriert wurde, besser ist als gar keine Firewall, wenn es wirklich darum geht, ein Netzwerk bspw. an das Internet anzubinden.

Einstufige und mehrstufige Firewalls

Eine mehrstufige Firewall ist am einfachsten mit einer mittelalterlichen Burg vergleichbar. Sie wird nicht nur von einer Mauer geschützt, sondern enthält mehrere Verteidigungsanlagen hintereinander. Wird eine durchbrochen, ist ein Einbruch noch nicht möglich.
Eine mehrstufige Firewall besteht nun aus mehreren einzelnen Firewallsystemen, die hintereinander arbeiten. Kann ein Angreifer die erste überwinden, wird er sich mit dem nächsten System konfrontiert sehen.
Solche eine mehrstufige Firewall hat Vor- und Nachteile

- Besserer Schutz durch mehrere Sicherheitssysteme
- Größerer Schutz vor Softwarefehlern eines Herstellers.
  Fällt ein System wegen eines Softwarefehlers aus, wird das die anderen Systeme nicht betreffen.
- Mehrstufige Firewallsysteme können nicht so leicht durch unwissende Mitarbeiter außer Kraft gesetzt werden.
- Durch die Verbindung von mehreren Systemen ist eine mehrstufige Firewall allerdings teuerer und aufwendiger zu administrieren.

Mehrstufige Firewallsysteme kommen auch zum Einsatz, wenn nicht nur zwei Netze miteinander verbunden werden, sondern Inselnetze entstehen, die andere Aufgaben haben und vielleicht aus dem Internet erreichbar sein sollen (z.B. für einen Webserver).

Räumliche Positionierung einer Firewall

Eine Firewall sollte nicht dadurch umgangen werden können, dass jemand Zugriff auf den Computer hatte und die Firewall deaktiviert hat. Da viele Angriffe mit Hilfe von Mitarbeitern begangen werden, muss die Firewall räumlich geschützt werden und nur wenige Mitarbeiter dürfen Zugriff ihr haben.

Komponenten der Firewall

Eine Firewall kann aus verschiedenen Komponenten bestehen. Diese bieten auf unterschiedliche Art und Weise Schutz vor Angriffen.

- **Paketfilter**
  Eine *Paketfilter* ist eine Komponente, die bestimmte Netzwerkpakete durchlässt oder blockiert. Dabei werden die Pakete anhand der Quell- und Zieladressen, der verwendeten Ports und des Protokolls und anhand interner Flags in den Paketen gefiltert. Ein Paketfilter überprüft allerdings nicht die übermittelten Daten, sondern nur die Adresse, den Absender und den verwendeten Port des Pakets. Diese Filter werden in Form von Regeln in die Firewall implementiert, die bestimmen, ob ein passendes Paket durchgelassen oder blockiert wird.
  Eine sinnvolle Regelung blockiert alle Pakete und lässt nur ausgewählte passieren. Die weniger sinnvolle Regelung lässt generell alle Pakete durch und blockiert nur einige ausgewählte. Das kann dazu führen, dass Protokolle vergessen wurden, die dann nicht in der Firewall blockiert werden.
- **Dynamische Filter**
  Ein Paketfilter kann neben statischen Regeln auch dynamische Filter verwenden. Diese passen sich an besondere Umstände an und blockieren z.B. bei einem erkannten Angriff die IP-Adressen der angegriffenen oder angreifenden Computer.
- **Application Gateways**
  Während Paketfilter sich die übertragenden Daten nicht anschauen, beschäftigt sich ein Application Gateway mit dem Inhalt der Pakete. Solche Gateways wenden auf die Paketinhalte Regeln an, die bestimmte Dinge verhindern. Durch ein Application Gateway können auch Übertragungen kontrolliert werden, die nicht mehr die normalen Verbindungskanäle verwenden. Durch die Trennung der Netzwerke auf der Anwendungsebene, wird ein direkter Datenaustausch zwischen einem internen und einem externen Computer verhindert. Beide Computer tauschen nun Daten mit dem Gateway aus und dieses wird den Austausch verhindern, wenn die Daten eine Abnormalität aufweisen.

Überwachung der Firewall

Eine Firewall muss ständig überwacht werden, damit Angriffe erkannt und evtl. reagiert werden kann. Dabei muss zwischen wirklichen Angriffen und dem einfachen Scannen von Ressourcen unterschieden werden, da solche Scans fast pausenlos aus dem Internet auf jedem angebundenen System durchgeführt werden. Aber auch solche Scans müssen aufgezeichnet werden, um diese Aufzeichnungen im Falle eines Angriffs zur Hand zu haben.
Ein gutes Firewallsystem wird solche Protokolle analysieren und bei Bedarf einen Administrator verständigen. Aber auch interne Fehler der Firewall und andere Ereignisse müssen automatisch protokolliert werden und diese Protokolle müssen vor einem Angreifer geschützt werden, damit dieser nicht seine Spuren verwischen kann.

Fallen

Um einem Angreifer das Leben so schwer wie möglich zu machen, können Fallen eingesetzt werden. Eine solche Falle besteht aus einem oder mehreren interessant aussehenden Systemen, die weniger geschützt sind. Diese Systeme sind völlig getrennt von den wirklichen Systemen und enthalten nur nutzlose Informationen und sind dazu gedacht, einen Angreifer von den wirklichen Systemen abzulenken. Außerdem kann ein Einbruch in solch eine Falle entdeckt werden und es können Maßnahmen ergriffen werden, bevor der Angreifer in die wichtigen Systeme eingebrochen ist, so dass man etwas mehr Zeit gewinnt.

5.4.3 Einbruchserkennende Systeme (Intrusion Detection Systeme, IDS)

Intrusion Detection Systeme (IDS) sind ein wirkungsvoller Schutz für das interne Netzwerk. Auch wenn eine Firewall das Netzwerk vor externen Angriffen schützen kann, kann ein interner Angreifer nicht durch eine Firewall aufgehalten werden. Ein IDS-System überwacht nun einen internen Server oder ein internes Netzwerk und wartet auf ungewöhnliche Aktivitäten oder überprüft die Einstellungen auf einem Server.

Hostbasierte IDS-Systeme

IDS-Systeme dieser Kategorie erkennen ungewöhnliche Aktivitäten auf einem Computer und analysieren Protokolle, Zugriffsrechte und Dateien oder Programme auf dem System auf Anzeichen für einen Angriff.

Netzwerkbasierte IDS-Systeme

Diese verwenden Agenten, die im Netzwerk installiert sind und überwachen das Netzwerk, indem sie die übertragenden Daten abhören. Wird ein ungewöhnlicher Datenstrom entdeckt, kann das IDS-System den Administrator verständigen und mit ähnlichen Mitteln, die auch ein Angreifer verwenden würde, die Netzwerkverbindung unterbrechen, indem die Übertragung übernommen und dann beendet wird.
Ungewöhnliche Aktivitäten im Netzwerk können z.B. vermehrt auftretende Netzwerkscans sein; ein IDS-System vergleicht die Netzwerkaktivitäten mit einem statistisch ermittelten Normalzustand oder mit einem Regelwerk, das erlaubte Aktivitäten definiert.
Einige IDS-Systeme können außerdem mit einer entsprechenden Firewall (meist vom gleichen Hersteller) kooperieren und die Konfiguration der Firewall aktiv bei einem entdeckten Angriff ändern.

6 Zusammenfassung

Windows 2000 wurde in den bisherigen Kapiteln analysiert. Das Betriebssystem enthält in der evaluierten Version einige neue Dienste und Komponenten, die die Sicherheit erhöhen und das Einsatzgebiet erweitern sollen.
Durch die vielseitigen Anwendungsmöglichkeiten von Windows 2000 kann die Frage nach der Sicherheit des Systems nur abhängig vom Einsatzgebiet beantwortet werden. Die Definition einer Sicherheitsrichtlinie, die nicht nur einen Computer, sondern das gesamte Netzwerk und darüber hinaus auch das gesamte Unternehmen betrifft, ist die Grundlage für ein sicheres Gesamtsystem. Windows 2000 stellt für die Anwendung dieser Sicherheitsrichtlinie in einem Computernetzwerk einige Werkzeuge bereit, mit denen sie sich in homogenen Windows 2000 Umgebungen durchsetzen lässt. Speziell dafür wurden die Sicherheitsvorlagen und Gruppenrichtlinien im System integriert, die eine Grundlage für sichere Einstellungen bieten, aber an spezielle Bedürfnisse angepasst werden sollten, um der Sicherheitsrichtlinie in einem Unternehmen gerecht zu werden.

Entscheidend für die Sicherheit eines Systems sind nicht nur die Sicherheitsrichtlinien, die im System abgebildet werden müssen, sondern auch das eventuelle Vorhandensein von Sicherheitsproblemen und deren schnelle Behebung. Microsoft hat sich für eine recht offene Sicherheitspolitik entschieden und gibt Interessenten die Möglichkeit, sich über aktuelle Sicherheitsprobleme zu informieren. Diese Sicherheitspolitik endet nicht bei der Information über aktuelle Probleme, sondern geht mit der schnellen Veröffentlichung von Softwareupdates einher, die diese Fehler beheben. Es ist jedem Administrator, der eine gewisse Verantwortung für die Sicherheit seiner Systeme übernimmt, selbst überlassen, sich zu informieren und aktiv etwas für die Sicherheit dieser Systeme beizutragen.

Die interne Sicherheit von Windows 2000 und einem Windows 2000 Netzwerk wird durch eine Reihe von neuen Diensten und Protokollen, die teilweise auf vorhandenen Internetstandards basieren, gewährleistet und kann nicht nur die einzelnen Computer, sondern auch den Datenverkehr in einem Netzwerk sichern. Die Verwendung von standardisierten Internetprotokollen erleichtert die Einbindung der Windows 2000 Sicherheit in andere Systeme und ermöglicht zumindest eine teilweise Überprüfung der Sicherheit des Systems, da diese Protokolle öffentlich zugänglich sind.

Insgesamt kann Windows 2000 durch seine neuen Sicherheitsdienste sehr sicher konfiguriert werden und es ist mehr eine Sache des Wollens und nicht des Könnens, ob diese angewendet werden oder nicht.

7 Ausblick

Diese Arbeit stellt eine Analyse der Sicherheitskomponenten des Microsoft Windows 2000 Betriebssystems dar. Sie gibt Interessenten einen Überblick über die Arbeitsweise des Betriebssystems und zeigt Lösungen für bekannte Sicherheitsprobleme und vorhandene Schwachstellen des Systems auf.

Durch die Komplexität der möglichen Anwendungen, die Windows 2000 bietet, wäre die Annahme, dass diese Arbeit den gesamten Bereich abdecken kann, völlig utopisch. Für eine ausführliche Beschreibung der Sicherheitsfunktionen, -protokolle und -dienste wäre der Umfang um ein Vielfaches höher.

Der nächste Schritt wäre die Erstellung einer detaillierten Beschreibung zur Konfiguration sicherer Windows 2000 Systeme für diverse Anwendungsgebiete. Dazu könnte auch die genaue Beschreibung der Konfiguration von verwendeten Protokollen, Diensten und Richtlinien gehören.

Die Veröffentlichung von Microsoft Windows XP im Herbst 2001 eröffnet weitere Möglichkeiten, diese Arbeit fortzusetzen.

8 Verzeichnisse

8.1 Allgemeines Literaturverzeichnis

[SOL00] D. Solomon, M. Russinovich: Inside Microsoft Windows 2000, Microsoft Press, 3.Auflage 2000, ISBN 3-86063-630-8

[ISS00] Internet Security Systems Inc.: Microsoft Windows 2000 Sicherheit, Microsoft Press, 2000, ISBN 3-86063-622-7

[LEE00] T. Lee, J. Davies: Microsoft Windows 2000 TCP/IP-Protokolle und -Dienste, Microsoft Press, 2000, ISBN 3-86063-620-0

[SCH01] J. Schmidt: windows 2000 security, Markt+Technik, 1999, ISBN 3-8272-5683-6

[BRI01] G. O'Brien: internet information server 5.0, Markt+Technik, 2001, ISBN 3-8272-6019-1

[NOR01] S. Norberg: Securing Windows NT/2000 Servers for the Internet, O'Reilly, 1.Auflage 2001, ISBN 1-56592-768-0

[KUR01] G. Kurtz, S. McClure, J. Scambray: Das Anti-Hacker-Buch, mitp-Verlag, 2.Auflage 2001, ISBN 3-8266-0670-1

[ANO00] anonymous: linux hacker's guide, Markt+Technik, 2000, ISBN 3-8272-5622-4

[STR99] S. Strobel: Firewalls, dpunkt.verlag, 2.Auflage 1999, ISBN 3-932588-49-5

[HAR99] C. Hartmann: Leitfaden für einen Sicherheitsplan für verteilte Desktop-Umgebungen in großen Unternehmensnetzwerken, Fachbereich Informatik, Universität Hamburg, 1999

8.2 Microsoft-Word-Dokumente, heruntergeladen von http://www.microsoft.com

Die Microsoft-Word-Dokumente wurden im PDF-Format auf der beiliegenden CD unter dem Quellennamen gespeichert.

[DOC01] Joel Scambray: Fragen an uns ... Sicherheit, März 2001, Microsoft Technet

[DOC02] Joel Scambray: Fragen an uns ... Sicherheit, Juni 2001, Microsoft Technet

[DOC03] Whitepaper, Grundlagen der Kryptografie und der Infrastruktur öffentlicher Schlüssel (PKI), Microsoft Technet

[DOC04] Whitepaper, Eine Einführung in die Public Key Infrastructure von Windows 2000, Microsoft Technet

[DOC05] Whitepaper, Einmalige Anmeldung (Single Sign-On, SSO) an Windows 2000-Netzwerken, Microsoft Technet

[DOC06] James Morey: Im Labyrinth der Berechtigungen, Microsoft Technet

[DOC07] Interoperabilität von Windows 2000-RSVP-und Kerberos-Benutzerauthentifizierung, Microsoft Technet

[DOC08] Microsoft Corporation: Kerberos 5 (krb5 1.0)-Interoperabilität, Microsoft Technet

[DOC09] Scott Culp: Microsoft-Sicherheitspatches, Microsoft Technet

[DOC10] Schrittweise Anleitung zu Internet Protocol Security (IPSec), Microsoft Technet

[DOC11] Craig Clayton: Sicherheit von Windows 2000 in einer E-Commerce-Umgebung, Microsoft Technet

[DOC12] Christopher Benson, Inobits Consulting (Pty) Ltd: Sicherheitsplanung, Microsoft Technet

[DOC13] Tom Dodds, Ken Pfeil: Sicherheitsüberlegungen für Endsysteme, Microsoft Technet

[DOC14] Whitepaper, Technische Übersicht über die Sicherheit von Windows 2000, Microsoft Technet

8.3 Internet-Dokumente

Die Internet-Dokumente wurden im PDF-Format auf der beiliegenden CD unter dem Quellennamen gespeichert.

[URL01] Windows 2000 Distributed Security Features Security Services, http://www.microsoft.com/TechNet/prodtechnol/windows2000serv/evaluate/secover.asp

[URL02] White Paper, Default Access Control Settings in Windows 2000, http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/featusability/secdefs.asp

[URL03] White Paper, Windows 2000 Security Technical Overview, http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/sectech.asp

[URL04] Chapter 1 - Overview of Microsoft Windows 2000 System Administration, http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/featusability/c01w2kad.asp

[URL05] Joel Scambray, Ask Us About... Security, November 2000, EFS Best Practices, http://www.microsoft.com/technet/columns/security/auas1100.asp

[URL06] White Paper, Encrypting File System for Windows 2000, http://www.microsoft.com/TechNet/prodtechnol/windows2000serv/deploy/confeat/nt5efs.asp

[URL07] IPSec Does Not Secure Kerberos Traffic Between Domain Controllers, http://support.microsoft.com/support/kb/articles/Q254/7/28.asp

[URL08] Joel Scambray, Ask Us About... Security, May 2000, Password length, http://www.microsoft.com/technet/columns/security/auas042400.asp

[URL09] Joel Scambray, Ask Us About... Security, April 2000, The Talk of the Town: DDoS, http://www.microsoft.com/technet/columns/security/auas032700.asp

[URL10] How to Restore an Encrypting File System Private Key for Encrypted Data Recovery, http://support.microsoft.com/support/kb/articles/Q242/2/96.asp

[URL11] Joel Scambray, Ask Us About... Security, September 2000, Using IPSec filters, http://www.microsoft.com/technet/columns/security/au091100.asp

[URL12] Joel Scambray, Ask Us About... Security, February 2001, What's the best tool to dump ACLs?, http://www.microsoft.com/technet/

columns/security/auas0201.asp

[URL13] Joel Scambray, Ask Us About... Security, March 2001, http://www.microsoft.com/technet/columns/security/auas0301.asp

[URL14] New Security Tool for Encrypting File System,cipher.exe, http://www.microsoft.com/technet/itsolutions/security/tools/cipher.asp

[URL15] Qfecheck.exe Verifies the Installation of Windows 2000 Hotfixes, http://support.microsoft.com/support/kb/articles/Q282/7/84.asp

[URL16] Use QChain.exe to Install Multiple Hotfixes with Only One Reboot, http://support.microsoft.com/support/kb/articles/Q296/8/61.asp

[URL17] Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool Is Available, http://support.microsoft.com/support/kb/articles/q303/2/15.asp

[URL18] Marc Ruef, Die Sicherheit von Windows 2000, http://www.trojaner-info.de/faq/anleitungen/die%20sicherhei1.htm

[URL19] Kerberos Autentifikation, http://wwwbs.informatik.htw-dresden.de/svortrag/ai95/Bindrich/kerberos.html

[URL20] EFS tools you gotta have, trainAbility, http://www.trainability.com/free/encryption2.htm

[URL21] Adding & removing accessories & utilities, trainAbility, http://www.trainability.com/free/accinstall.htm

[URL22] Yale University Windows 2000 Workstation Security Guidelines, http://www.yale.edu/its/security/Procedures/Securing/NT/w2k/

[URL23] Petter Nordahl, Offline NT Password & Registry Editor, Bootdisk, http://home.eunet.no/~pnordahl/ntpasswd/bootdisk.html

[URL24] Petter Nordahl, Offline NT Password & Registry Editor, http://home.eunet.no/~pnordahl/ntpasswd/

[URL25] Arash Baratloo, Navjot Singh, Timothy Tsai, Transparent Run-Time Defense Against Stack Smashing Attacks http://www.avayalabs.com/project/libsafe/doc/usenix00/paper.html

[URL26] Aleph One, Smashing The Stack For Fun And Profit

[URL27] Alan O. Freier, Philip Karlton, Paul C. Kocher, The SSL Protocol Version 3.0

8.4 Internet Engineering Task Force, Request For Comment

Die RFC-Dokumente wurden als Text-Dateien auf der beiliegenden CD unter dem Quellennamen gespeichert.

[RFC0412] G. Hicks: User FTP Documentation

[RFC0793] Transmission Control Protocol, http://www.ietf.org/rfc/rfc0793.txt

[RFC0821] Jonathan B. Postel: SIMPLE MAIL TRANSFER PROTOCOL, http://www.ietf.org/rfc/rfc.txt

[RFC0822] David H. Crocker: STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES, http://www.ietf.org/rfc/rfc0822.txt

[RFC0850] Mark R. Horton: Standard for Interchange of USENET Messages, http://www.ietf.org/rfc/rfc0850.txt

[RFC0822] P. Mockapetris: DOMAIN NAMES - CONCEPTS and FACILITIES, http://www.ietf.org/rfc/rfc0822.txt

[RFC0883] P. Mockapetris: DOMAIN NAMES - IMPLEMENTATION and SPECIFICATION, http://www.ietf.org/rfc/rfc0883.txt

[RFC0959] J. Postel, J. Reynolds: FILE TRANSFER PROTOCOL (FTP), http://www.ietf.org/rfc/rfc0959.txt

[RFC0977] Brian Kantor, Phil Lapsley: Network News Transfer Protocol, http://www.ietf.org/rfc/rfc0977.txt

[RFC1001] NetBIOS Working Group: PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: CONCEPTS AND METHODS, http://www.ietf.org/rfc/rfc1001.txt

[RFC1002] NetBIOS Working Group: PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: DETAILED SPECIFICATIONS, http://www.ietf.org/rfc/rfc1002.txt

[RFC1034] P. Mockapetris: DOMAIN NAMES - CONCEPTS AND FACILITIES, http://www.ietf.org/rfc/rfc1034.txt

[RFC1035] P. Mockapetris: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION, http://www.ietf.org/rfc/rfc1035.txt

[RFC1036] M. Horton, R. Adams: Standard for Interchange of USENET Messages, http://www.ietf.org/rfc/rfc1036.txt

[RFC1179] L. McLaughlin III: Line Printer Daemon Protocol, http://www.ietf.org/rfc/rfc1179.txt

[RFC1510] J. Kohl: The Kerberos Network Authentication Service (V5), http://www.ietf.org/rfc/rfc1510.txt

[RFC1591] J. Postel: Domain Name System Structure and Delegation, http://www.ietf.org/rfc/rfc1591.txt

[RFC1635] P. Deutsch, A. Emtage, Bunyip, A. Marine: How to Use Anonymous FTP, http://www.ietf.org/rfc/rfc1635.txt

[RFC1777] W. Yeong, T. Howes, S. Kille: Lightweight Directory Access Protocol, http://www.ietf.org/rfc/rfc1777.txt

[RFC1823] T. Howes, M. Smith: The LDAP Application Program Interface, http://www.ietf.org/rfc/rfc.txt

[RFC1945] T. Berners-Lee, R. Fielding, H. Frystyk: Hypertext Transfer Protocol -- HTTP/1.0, http://www.ietf.org/rfc/rfc1945.txt

[RFC1964] J. Linn: The Kerberos Version 5 GSS-API Mechanism, http://www.ietf.org/rfc/rfc1964.txt

[RFC1995] M. Ohta: Incremental Zone Transfer in DNS, http://www.ietf.org/rfc/rfc1995.txt

[RFC2069] J. Franks, P. Hallam-Baker, J. Hostetler, P. Leach, A. Luotonen, E. Sink, L. Stewart: An Extension to HTTP : Digest Access Authentication, http://www.ietf.org/rfc/rfc2069.txt

[RFC2078] J. Linn: Generic Security Service Application Program Interface, Version 2, http://www.ietf.org/rfc/rfc2078.txt

[RFC2109] D. Kristol, L. Montulli: HTTP State Management Mechanism, http://www.ietf.org/rfc/rfc2109.txt

[RFC2131] R. Droms: Dynamic Host Configuration Protocol, http://www.ietf.org/rfc/rfc2131.txt

[RFC2132] S. Alexander, R. Droms: DHCP Options and BOOTP Vendor Extensions, http://www.ietf.org/rfc/rfc2132.txt

[RFC2136] P. Vixie, S. Thomson, Y. Rekhter, J. Bound: Dynamic Updates in the Domain Name System (DNS UPDATE), http://www.ietf.org/rfc/rfc2136.txt

[RFC2196] B. Fraser: Site Security Handbook, http://www.ietf.org/rfc/rfc2196.txt

[RFC2246] T. Dierks, C. Allen: The TLS Protocol Version 1.0, http://www.ietf.org/rfc/rfc2246.txt

[RFC2251] M. Wahl, T. Howes, S. Kille: Lightweight Directory Access Protocol (v3), http://www.ietf.org/rfc/rfc2251.txt

[RFC2411] R. Thayer: IP Security Document Roadmap, http://www.ietf.org/rfc/rfc2411.txt

[RFC2565] R. Herriot, Ed., S. Butler, P. Moore, R. Turner: Internet Printing Protocol/1.0: Encoding and Transport, http://www.ietf.org/rfc/rfc2565.txt

[RFC2566] R. deBry, T. Hastings, R. Herriot, S. Isaacson, P. Powell: Internet Printing Protocol/1.0: Model and Semantics, http://www.ietf.org/rfc/rfc2566.txt

[RFC2616] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. MasinterP. Leach, T. Berners-Lee: Hypertext Transfer Protocol -- HTTP/1.1, http://www.ietf.org/rfc/rfc2616.txt

8.5 Microsoft Security Bulletin-Dokumente

Die Microsoft Security Bulletin-Dokumente wurden im PDF-Format auf der beiliegenden CD unter dem Quellennamen gespeichert.

[MSJJ-NR] Die Microsoft Security Bulletin Dokumente verwenden eine eigene Nummerierung, die beibehalten wurde.
Dabei bezeichnet JJ das Jahr der Veröffentlichung und NR die laufende Nummer innerhalb des Jahres.

8.6 Abbildungsverzeichnis

8.7 Tabellenverzeichnis