Hilfsmittel zu Windows Server 2003

Dieses Dokument enthält konkrete Implementierungshinweise, die sich auf Maßnahmen des IT-Grundschutz Bausteins **B 3.108 Windows Server 2003** beziehen. Es soll als Orientierungshilfe für die Implementierung der Maßnahmen des Bausteins dienen.

Inhaltsverzeichnis

1 Migration eines Servers von einer früheren Windows-Version nach Windows Server 2003

Eine Migration von Windows NT4.0 Server oder Windows 2000 Server auf die Betriebssystemplattform Windows Server 2003 bedeutet:

0. Auswechseln (neu installieren) des Betriebsystems
0. Neukonfigurieren des Betriebssystems
0. Übernahme bestehender Nutzdaten vom alten System in das neue

Zuerst Planung des Servers unter Windows Server 2003

Vor der Migration sollte das Zielszenario geplant worden sein, denn in den meisten Fällen ist das Zielszenario aufgrund von Konsolidierungs- und Restrukturierungseffekten sowie durch neue Funktionen nicht identisch mit dem Ursprungsszenario. Für den einzelnen Server sollte also zuerst eine Planung wie für einen neuen Server unter Windows Server 2003 durchgeführt werden. Als nächstes sollten die Bedingungen des Übergangs analysiert und festgelegt werden, z. B.:

- Wird die bestehende Server-Hardware weiterverwendet oder kommt ein alternativer (neuer) Server zum Einsatz?
- Kann oder muss das Zielsystem identische Infrastrukturparameter haben (z. B. Name, IP-Adresse)? Dies ist hauptsächlich von den Anwendungen und Diensten abhängig, die auf dem Server laufen. Es müssen also deren Betriebsbedingungen analysiert werden.
- Soll bzw. darf sich die Mitgliedschaft in der Active-Directory-Domäne ändern, z. B. neue Domäne?
- Welche Konten und Berechtigungen sind zum Betrieb der Serverdienste- und Anwendungen vorher und hinterher notwendig? Wie sollen diese im Zielsystem bereitgestellt werden?
- Welche Ausfallzeiten des betrachteten IT-Systems sind tolerierbar?
- Ist aus Ressourcensicht (z. B. zeitlich und personell) sowie aus Sicht der Verfügbarkeitsanforderung an die bisherigen bzw. neuen Funktionen eine Migration in einem Schritt vertretbar oder muss ein Übergangsszenario geschaffen werden, das für begrenzte Zeit einen eingeschränkten Produktivbetrieb ermöglicht?

Generell sollten diese Überlegungen darauf ausgerichtet sein, ein direktes Aktualisieren des alten Systems auf Windows Server 2003 mittels Setup-Programm zu vermeiden!

Neuinstallation vorziehen

Das aus Sicherheitssicht optimale Szenario ist die Neuinstallation eines Windows-Server-2003-Systems, das Konfigurieren gemäß den aktuellen Richtlinien und Vorlagen, rollenspezifische Konfiguration und schließlich die Datenübernahme entweder direkt vom alten System oder aus der aktuellen Datensicherung.

Wenn das geplante Migrationszenario dennoch ein direktes Aktualisieren eines Servers (engl. Upgrade) enthält, dann müssen auf dem betroffenen Server kontrollierte Bedingungen geschaffen werden. Die folgenden Abschnitte gehen auf Aspekte einer Aktualisierung unter kontrollierten Bedingungen näher ein.

Das Windows-Server-2003-Setup-Programm bietet die Aktualisierungsfunktion, um den Umstieg zu erleichtern und dadurch Kosten für den Migrationsvorgang zu sparen. Diese Variante wird *In-Place-Upgrade* genannt. Sie ist optimiert auf bestimmte vom Hersteller favorisierte Ursprungsszenarien und -konfigurationen. Die Optimierung beschränkt sich verständlicherweise auf Windows-eigene Funktionen. Um einen möglichst reibungslosen Betrieb von Windows Server 2003 in den alten Infrastrukturen zu ermöglichen, ist Standardkonfiguration der Sicherheitseinstellungen von Windows Server 2003 noch konservativer als bei einer Neuinstallation des Systems. Die resultierenden Einstellungen hängen von der Windows-Version und dem Service Pack des Ursprungssystems ab. Viele sicherheitsrelevante Einstellungen, die auf dem Ursprungssystems individuell angepasst wurden, werden auf das Zielsystem unter Windows Server 2003 übertragen, hierbei wird auch von der Übernahme von "Altlasten" gesprochen. Es ist praktisch nur schwer möglich, alle relevanten Parameter zu analysieren, vorherzusagen und die Konformität des Zielsystems mit den aktuellen Anforderungen für Windows Server 2003 zu gewährleisten.

Kontrollierte Upgrade-Bedingungen

Wie können dennoch möglichst kontrollierte Bedingungen für den Aktualisierungsvorgang hergestellt werden?

Die Maßnahme M 4.283 *Sichere Migration von Windows NT 4 Server und Windows 2000 Server auf Windows Server 2003* gibt hierfür grundsätzliche Hilfestellungen und Vorgaben für Planung und Durchführung.

Nachfolgend werden beispielhaft bestimmte Vorgehensweisen aufgezeigt, die für kontrollierte Bedingungen beim Upgrade sorgen können. Sie sind nicht allgemeingültig sondern dienen zur Orientierung.

Zuerst sollte der vorhandene Server analysiert und es sollte entschieden werden, welche Funktionen, Rollen und Server-Anwendungen überhaupt in den Upgrade-Vorgang des Betriebssystems mit einbezogen werden sollen. Alle nicht unbedingt benötigten sollten in der Folge vom Upgrade-Vorgang ausgeschlossen und unter Windows Server 2003 neu installiert werden. Hierzu sollten herstellerspezifische Unterlagen zu den Softwarekomponenten konsultiert werden, um das Verhalten vorherzusagen und die Notwendigkeit zu bestimmen. Für viele wichtige Windows-Komponenten stellt der Hersteller zu diesem Zweck Bereitstellungs- und Migrationsleitfäden kostenlos zur Verfügung (die entsprechende Sammlung heißt *Windows Deployment and Resource Kits*).

Es sollten möglichst wenige Funktionen, Rollen und Server-Anwendungen auf einem Server migriert werden. Ein "Multi-Funktions-Server" ist für das *In-Place-Upgrade*-Verfahren ungeeignet.

Separater Upgrade-Server

Verwendung eines separaten Upgrade-Servers

Wann immer es möglich ist, sollte ein dedizierter Upgrade-Server verwendet werden. Das ist ein separater Server, auf dem die ursprüngliche (alte) Version von Windows neu installiert und später aktualisiert wird. Es sollte vorher entschieden werden, ob der Upgrade-Server der endgültige Zielserver sein wird oder ob es sich um einen Interimsserver (temporärer Server) handelt.

Auf dem Upgrade-Server werden nur genau die benötigten Windows-Funktionen aktiviert und es werden die für das Upgrade mindestens

erforderlichen Service Packs und Patches installiert. Zusatzsoftware des Herstellers oder Drittherstellern ist nur zu installieren, wenn die Software aus Kompatibilitätsgründen oder Gründen der Datenübernahme dies unbedingt erfordert. Ansonsten ist das Windows-System so nah wie möglich am Installationsstandard zu halten.

Dieses Verfahren profitiert von den infrastrukturellen Fähigkeiten bestimmter Serverkomponenten, um Informationen bzgl. der Organisation, Struktur und/oder zum Betriebsstatus derselben auf andere Server zu übertragen. Bei Domänencontrollern und Namensservern sind das bspw. Namensbereiche, Sicherheitskontexte oder Domäneneinträge. Bei manchen Komponenten kann es hilfreich sein, solche Informationen manuell zu übertragen, evtl. zusammen mit den Nutzdaten. Diese Vorgehensweise ist z. B. bei Webseiten oder Webapplikationen, die in den *Internet Information Services* nutzen, sinnvoll.

Sobald alle Vorbereitungen auf dem Upgrade-Server getroffen worden sind, wird das Windows-Server-2003-Setup-Programm von der Installationsquelle gestartet. Es migriert die vorhandene Funktionalität und die vorhandenen Informationen während des Ugrade-Vorgangs ohne die Möglichkeit des Benutzereingriffs. Wenn es sich bei dem Upgrade-Server um das endgültige Zielsystem handelt, werden nach dem Upgrade die vorgesehenen Server-Anwendungen installiert und konfiguriert. Handelt es sich um einen Interimsserver, wird nach dem Upgrade das eigentliche Zielsystem mit Windows Server 2003 aufgesetzt (entweder auf der ursprünglichen oder auf neuer Hardware). Somit wird eine homogene Umgebung geschaffen und die Informationen des Interimsserver können auf das Zielsystem übernommen werden. Das Zielsystem nimmt dann seinen produktiven Betrieb auf.

Zum Schluss muss gegebenenfalls der Interimsserver deinstalliert werden. Für die Deinstallation der Software müssen die Unterlagen und Hinweise des Herstellers beachtet werden. Es ist zu empfehlen, jede Komponente einzeln zu deinstallieren und ordnungsgemäß aus der Organisation bzw. der Struktur zu entfernen, damit keine so genannten "Leichen" zurückbleiben. Sofern der Interimsserver Mitglied einer Domäne ist, muss er aus der Domäne entfernt werden, oder die Vertrauensstellung muss aufgelöst werden.

Upgrade eines produktiven Servers

Upgrade eines produktiven Servers

Dieses Verfahren stellt hohe Anforderungen an die Konstitution des Ursprungssystems, insbesondere wenn der Server nach der Aktualisierung dauerhaft produktiv eingesetzt werden soll. Häufig empfiehlt sich dies nur als Übergangszenario, der aktualisierte Server wird in einer weiteren Migrationsstufe durch einen neuen Server abgelöst. Das Verfahren kommt für Server in Frage, die sehr aufwendig konfiguriert wurden und deren Einstellungen schwer zu reproduzieren sind. Häufig sind das kritische Systeme, die keine längeren Ausfallzeiten ermöglichen oder kritische Informationen enthalten, beispielsweise Stammzertifizierungsstellen. Bei der Analyse des Ursprungssystems sollte überprüft werden, ob das System ordnungsgemäß konfiguriert und administriert wurde, sich nahe an den Standardeinstellungen befindet und möglichst wenige Altlasten enthält. Vor dem Upgrade sollten alle Funktionen, Programme und Werkzeuge soweit wie möglich deaktiviert bzw. deinstalliert werden, die auf dem Zielsystem nicht unbedingt erforderlich sind. Meist gibt es für Windows Server 2003 neuere

Versionen dieser Programme, die nach dem Upgrade neu installiert werden können.

Es sollte auch überlegt werden, bestimmte Funktionen bzw. Windows-Komponenten vom zu aktualisierenden Server auf einen separaten Upgrade-Server auszulagern.

Sicherheitsvorlagen

Standardsicherheitseinstellungen von Windows 2000 Server verwenden

Ein zu aktualisierender Windows 2000 Server enthält möglicherweise restriktive Sicherheitseinstellungen, und möglicherweise existieren Sicherheitsvorlagen für den Windows 2000 Server. Es ist zu empfehlen, für diesen Server eine neue Sicherheitsvorlage auf einem Windows-Server-2003-System zu erstellen (siehe M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003*) und nach dem Upgrade einzuspielen und zu testen. Beim Erstellen der Vorlage sollten die bisherigen Sicherheitsparameter auf dem Ursprungsserver sowie die für die Windows-Server-2003-Umgebung festgelegten Parameter berücksichtigt werden. Vor dem Upgrade-Vorgang ist es zu empfehlen, alle Sicherheitsparameter möglichst auf die Standardwerte von Windows 2000 zu setzen. Eine Möglichkeit hierfür ist die Vorlagen-Datei *setup security.inf* im Verzeichnis *C:\WINNT\Security\Templates* des Windows 2000 Servers.

Administrative Vorlagen

Das Verhalten von administrativen Vorlagen beim Upgrade ist in M 2.368 *Umgang mit administrativen Vorlagen unter Windows Server 2003* beschrieben. Für vorhandene benutzerdefinierte Vorlagen empfiehlt es sich, diese testweise auf einem Windows-Server-2003-Testsystem einzuspielen und zusammen mit der für das Zielsystem geplanten Software zu testen.

Rollback-Szenario

Sicherung des Servers vor dem Upgrade

Der Upgrade-Vorgang kann fehlschlagen bzw. ein nicht wie gewünscht funktionierendes System erzeugen, selbst wenn der Server ordnungsgemäß vorbereitet wurde. Daher sollte unbedingt eine vollständige Datensicherung vom Server erstellt werden, bevor das Upgrade mittels des Windows-Server-2003-Setup-Programms gestartet wird. Die Datensicherung sollte den Zustand des Servers im Produktivbetrieb enthalten. Am besten sind hierfür Programme geeignet, die ein Festplattenabbild von der Systempartition erzeugen. Wird ein produktiver Server direkt aktualisiert, sollte in jedem Fall eine Übung zur Datenrekonstruktion und Wiederherstellung des Systems durchgeführt werden, um die mögliche Gesamtausfallzeit des Systems abschätzen zu können. Auch bei einem separaten Upgrade-Server sollte das Rollback funktionieren, um diesen auch nach einem Fehlschlag wieder ordnungsgemäß deinstallieren und aus der Organisation lösen zu können.

Isoliertes Installationsnetz

Server während des Upgrades vom produktiven Netz trennen

Der Server sollte während der Aktualisierung vom Netz getrennt werden. Benötigt er während des Upgrades Ressourcen eines anderen Servers oder einen Domänencontroller, so sind diese in einem isolierten Installationsnetz zusammenzufassen. Insbesondere bei einer Domäne werden sonst sämtliche Änderungen in die Gesamtstruktur übertragen. Bei Fehlschlägen oder unerwarteten Effekten sind die Änderungen unter Umständen nicht mehr rückgängig zu machen.

Testlauf

Das isolierte Netz und das Rollback-Szenario ermöglichen einen Testlauf für den Upgrade-Vorgang. Tests sind häufig die einzige Möglichkeit, das Verhalten des Servers während und nach dem Upgrade vorherzusagen.

Testlauf vor Upgrade eines produktiven Servers

Wenn ein produktiver Server direkt aktualisiert wird, empfiehlt sich ein Testlauf auf einem identisch konfigurierten System. Das Testsystem kann mit Hilfe von Programmen zum Erzeugen von Festplattenabbildern erstellt werden.

Kostenlose Unterlagen des Herstellers

Die im Folgenden genannten Unterlagen können von der Internet-Seite des Herstellers mittels der Suchen-Funktion oder über verschiedene Distributionen des Herstellers bezogen werden.

Migration von Windows NT 4.0 Server nach Windows Server 2003

- Windows Server 2003 – Handbuch für die Bereitstellung: Migration von Windows NT 4.0 Domänen auf Windows Server 2003
- Windows Deployment and Resource Kit: Migrating from Windows NT Server 4.0 to Windows Server 2003

Migration von Windows 2000 Server nach Windows Server 2003

- Upgrading from Windows 2000 Server to Windows Server 2003

Migration von Applikationen auf eine Windows-Server-2003-Plattform

- Moving Windows NT 4.0 and Windows 2000 Applications to Windows Server 2003

Migration einer Zertifizierungsstelle

- Knowledge Base: Artikel 298138 How to move a certification authority to another server

2 RPC, SMB und LDAP unter Windows Server 2003

Folgende Sicherheitseinstellungen sind nach einer Standardinstalltion nicht gesetzt. Sie sollten überprüft und gegebenenfalls angepasst werden.

Start | *Systemsteuerung* | *Verwaltung* | *Lokale Sicherheitsrichtlinie,* dann *Lokale Richtlinien* | *Sicherheitsoptionen*

Pos.	Einstellung	Wert
1	Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)	Aktiviert
2	Domänenmitglied: Starker Sitzungsschlüssel erforderlich (Windows 2000 oder höher)	Aktiviert
3	Microsoft-Netzwerk (Client): Kommunikation digital signieren (immer)	Aktiviert
4	Microsoft-Netzwerk (Server): Kommunikation digital signieren (immer)	Aktiviert
5	Microsoft-Netzwerk (Server): Kommunikation digital signieren (wenn Client zustimmt)	Aktiviert
6	Netzwerksicherheit: Abmeldung nach Ablauf der Anmeldezeit erzwingen	Aktiviert
7	Netzwerksicherheit: Keine LAN Manager-Hashwerte für nächste Kennwortänderung speichern	Aktiviert
8	Netzwerksicherheit: LAN Manager-Authentifizierungsebene	5 (Nur NTLMv2-Antworten senden\LM & NTLM verweigern)
9	Netzwerksicherheit: Signaturanforderungen für LDAP-Clients	Signatur erforderlich
10	Netzwerksicherheit: Minimale Sitzungssicherheit für NTLM-SSP-basierte Clients (einschließlich sicherer RPC-Clients)	Alles aktivieren
11	Netzwerksicherheit: Minimale Sitzungssicherheit für NTLM-SSP-basierte Server (einschließlich sicherer RPC-Server)	Alles aktivieren
12	Microsoft-Netzwerk (Client): Unverschlüsseltes Kennwort an SMB-Server von Drittanbietern senden (besonders kritische Einstellung, daher immer überprüfen)	Deaktiviert (Standard)

0. *Start* | *Systemsteuerung* | *Verwaltung* | *Komponentendienste*
0. In der Konsole: *Komponentendienste* | *Computer* | *Arbeitsplatz*
0. *Eigenschaften* | *Standardeigenschaften* | *Standardauthentifizierungsebene* auf *Paketdatensicherheit* setzen

0. Einstellungen mit *OK* bestätigen

Kompatibilitätshinweise und geeignete Werkzeuge

Werkzeuge für andere Systemtypen, die eine Kompatibilität zu Windows-Server 2003-Umgebungen ermöglichen:

- MS Directory Service Client (DS-Client) für Windows 95/98/NT4
- Samba ab Version 3.0.21
- MS User Authentication Module (MSUAM) für MacOS ab Version 10.1

Der Clusterdienst und die *Routing and Remote Access Services* (RRAS) funktionieren erst ab Windows Server 2003 mit Service Pack 1 ordnungsgemäß mit NTLMv2. Die einfache CHAP-Authentisierung (Challenge Handshake Authentication Protocol) der RRAS-Dienste an einem Domänencontroller ist mit NTLMv2 nicht mehr möglich.

Auf Servern, die nur als Druckserver verwendet werden, kann die Sicherheitseinstellung *Microsoft-Netzwerk (Server): Kommunikation digital signieren (immer)* (Position 4 in der obigen Liste) deaktiviert bleiben, da Benutzer sonst die Druckerwarteschlange nicht einsehen können.

Aktivierung und Durchsetzung der Einstellungen

Aktivierungsreihenfolge

Die Aktivierungsreihenfolge der oben beschriebenen Sicherheitseinstellungen kann den Betrieb des Windows-Netzes negativ beeinflussen, z. B. ist möglicherweise keine Authentisierung mehr durchführbar. Als Orientierung für die Planung der Durchsetzung in einem bestimmten Bereich gilt das Prinzip:

erst Clients

↓

dann Mitgliedsserver

↓

zum Schluss Domänencontroller

Die Einstellungen für *Kommunikation digital signieren*, *Sitzungssicherheit*, *Authentifizierungsebene*, *Signaturanforderungen für LDAP* und *sicherer Kanal* sollten in getrennten und gegebenenfalls mehrfachen Durchläufen umgesetzt werden, um die Sicherheit stufenweise zu erhöhen.

Beispiel:

0. Durchlauf: Die jeweiligen Einstellungen nicht restriktiv setzen (z. B. mit dem Zusatz *wenn Server zustimmt* oder *wenn Client zustimmt*).
0. Durchlauf: Die jeweiligen Einstellungen restriktiv setzen (z. B. mit dem Zusatz *immer*).

Auf jeder Stufe eines Durchlaufs sollte das Ereignisprotokoll auf fehlgeschlagene Kommunikationsversuche hin untersucht und die Fehlerursache beseitigt werden, bevor die nächste Stufe umgesetzt wird. Details zu typischen Fehlermeldungen liefert unter anderem der *Microsoft*

Knowledge Base Artikel 823659 Revision 11 vom 9. Februar 2006 (oder eine späteren Revision).

3 Absichern von IP-Protokollen unter Windows Server 2003

TCP/IP-Einstellungen zum Schutz vor Denial-of-Service-Attacken

Einstellungen in der Registrierdatenbank des Servers:

Einstellung	Wert
`HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \AFD \Parameters \DynamicBacklogGrowthDelta`	10
`HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \AFD \Parameters \EnableDynamicBacklog`	1
`HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \AFD \Parameters \MaximumDynamicBacklog`	20000
`HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \AFD \Parameters \MinimumDynamicBacklog`	20
`HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \tcpip \Parameters \TcpMaxPortsExhausted`	5

Einstellungen der lokalen Richtlinie des Servers im *Sicherheitskonfigurations-Editor* (SCE) (siehe M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows 2003 Server*):

Start | *Systemsteuerung* | *Verwaltung* | *Lokale Sicherheitsrichtlinie* | *Lokale Richtlinie* | *Sicherheitsoptionen*

Einstellung	Wert	Einschränkung
MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	2 (Höchster Schutz; Source Routing ist vollständig deaktiviert)	-
MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)	0 (Deaktiviert)	keine automatische Umschaltung auf alternative Standardgatewa ys

MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	0 (Deaktiviert)	Server nicht als Autonomous System BoundaryRouter (ASBR) einsetzbar
MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers (Only recommended for servers)	1 (Aktiviert)	-
MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)	0 (Deaktiviert)	deaktiviert Internet Router Discovery Protocol (IRDP)
MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)	1 (Verbindungsunterbrechung, wenn ein SYN-Angriff erkannt wird)	-
MSS: (TcpMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged	3 (3, 6, & 9 Sekunden, halboffene Verbindungen werden nach 45 Sekunden beendet)	-
MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	3	-
MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds	300000	-

MSS steht hier für *Microsoft Solutions for Security* (Microsoft Sicherheitslösungen).

SynAttackProtect und *TcpMaxConnectResponseRetransmissions* sind ab Windows Server 2003 mit Service Pack 1 standardmäßig bereits aktiviert. Alle aufgelisteten Einstellungen haben in einer homogenen Windows-Umgebung keine funktionalen Auswirkungen (Ausnahmen siehe Spalte "Einschränkungen"). In einer heterogenen Umgebung allerdings muss die Kompatibilität der Einstellungen mit anderen IT-Systemen geklärt werden, z. B. anhand von Herstellerunterlagen der Systeme oder mit Hilfe von Tests.

Hinweise zu Kommunikationsprotokollen der Internetprotokoll-Suite

- **RPC, SMB/CIFS, NetBIOS over TCP/IP, LDAP**
  Das Steuerungsprotokoll *Remote Procedure Calls* (RPC), die Netz-Dateiprotokolle, *Server Message Block* (SMB) und *Common Internet File System* (CIFS), das Verzeichnisdienstprotokoll *Leightweight Directory Access Protocol* (LDAP) sowie NetBIOS (Peer-to-Peer-Basisdienste) sind integrale Bestandteile der Kommunikation zwischen Windows-Systemen. Sie sind tief in die Sicherheitsarchitektur von Windows Server 2003 eingebunden. Die Sicherheit dieser Protokolle kann über Sicherheitsrichtlinien-Einstellungen und andere Kontrollprogramme fein abgestimmt werden (siehe M 4.277 *Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows Server 2003*).

- **NTP/SNTP**
  Mit dem *Network Time Protocol* (NTP/SNTP) wird die Systemzeit synchronisiert. Eine Windows-Domänenumgebung mit Kerberos toleriert nur geringe Zeitabweichungen. Daher wird NTP/SNTP beim Domänenbeitritt automatisch konfiguriert. NTP/SNTP ist ebenfalls tief in die Sicherheitsarchitektur von Windows Server 2003 eingebunden. Allerdings ist die Synchronisation mit einer externen Zeitquelle sicherheitskritisch. Daher sollten nur interne, kalibrierte Zeitserver abgefragt werden. Interne Zeitserver können z. B. von Sicherheits-Gateways oder mit Hilfe von Funkuhren bereitgestellt werden.

- **WINS/DNS/DHCP**
  In einer Windows-Domänenumgebung basieren die essentiellen Infrastrukturdienste für Namensauflösung und Management von IP-Adressen vor allem auf dem *Domain Name System* (DNS) und dem *Dynamic Host Configuration Protocol* (DHCP). DNS und DHCP sind tief in die Sicherheitsarchitektur von Windows Server 2003 eingebunden. *Windows Internet Name Service* (WINS) diente vor allem in früheren Windows-Versionen zur Namensauflösung und ist aus Gründen der Kompatibilität zu älteren Windows-Versionen und Software von Drittherstellern in der Praxis häufig nicht verzichtbar. Es bringt jedoch Abstriche bei der Sicherheitskonfiguration mit sich. Die Maßnahme HM15 *Konfiguration der Infrastrukturdienste für DNS, DHCP und WINS unter Windows Server 2003* sollte umgesetzt werden.

- **SNMP**
  Das *Simple Network Management Protocol* (SNMP, SNMPv3) und *Remote Monitoring* (RMON) werden für Netzwerkmanagement-Systeme benötigt. Sie können z. B. in den Netzwerkmonitorprogrammen von Windows Server 2003 verwendet werden. Falls SNMP aktiviert werden soll, müssen wenigstens der Community-Name von *public* auf einen individuellen Namen geändert und konkrete Trap-Ziele angegeben werden. Da SNMP insgesamt unzureichende Sicherheitsfunktionen bietet, ist zu überlegen, das Netz auf einer tieferen OSI-Schicht abzusichern - z. B. mittels IPSec- und die Sicherheit gegen Kompromittierung von SNMP an den Grenzen und Übergangen des LAN generell sicherzustellen.

- **BOOTP, TFTP, PXE**
  Der *Remote Installation Service* (RIS) baut auf *Bootstrap Protocol* (BOOTP), *Trivial File Transfer Protocol* (TFTP), dem *Preboot Execution Environment* (PXE) Protokoll sowie DHCP auf. PXE ist ein Client/Server-Protokoll zum Booten von Clients ohne eigenes Betriebssystem. Der Einsatz von Windows Server 2003 als RIS-Server ist grundsätzlich kritisch, weil die Kommunikationspartner (d. h. die zu installierenden Computer) keine Windows-Clients sind, sondern nur rudimentär ausgestatte Netz-Boot-Umgebungen ohne Sicherheitsfunktionen. Die Kommuni- kation findet über diese unsicheren Protokolle statt und kann weder durch die standardmäßigen noch durch erweiterte Sicherheitsfunktionen von Windows Server 2003 abgesichert werden. Dementsprechend können die RIS-Dienste zwar konfiguriert und bereitgestellt werden, sollten aber nur im konkreten Bedarfsfall aktiviert und danach wieder deaktiviert werden. Weiterhin ist zu empfehlen, die Sicherheit an den Grenzen und Übergangen des LAN generell zu erhöhen und den erhöhten technischen und organisatorischen Aufwand von Remote-Installationsdiensten im IT-Sicherheitsmanagement zu berücksichtigen, z. B. in einer geeigneten Richtlinie für die lokale IT-Umgebung und durch ein geeignetes Betriebskonzept für Remote-Installationsdienste.

- **ICMP**
  Falls die Gefährdung G 5.50 *Missbrauch des ICMP-Protokolls* auch für den geschützten Netzbereich nach IT-Grundschutz als kritisch identifiziert wurde, dann sollte ICMP durch Verwendung der lokalen Windows-Firewall abgesichert werden. (siehe M 4.280 *Sichere Basiskonfiguration von Windows Server 2003*).

- **Internetprotokolle der Komponente *Anwendungsserver***
  Grundlegende Vorkehrungen zum Absichern der Authentisierung von HTTP/HTTPS-, SMTP- und NNTP-Zugriffen sind der Maßnahme M 4.282 *Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003* zu entnehmen. Windows Server 2003 bietet für SMTP und NNTP die Einbindung eines Sicherheitszertifikats und die Kommunikation über einen sicheren Kanal an. Der Einsatz eines sicheren Kanals (also Verwendung von Verschlüsselung) ist zu empfehlen. Bei FTP stehen keine Sicherheitsfunktionen für die Verschlüsselung von Kennwort und Nutzdaten zur Verfügung. Hier sollte überlegt werden, einen sicheren Kanal durch Software von Drittherstellern zu verwenden, beispielsweise den SFTP-Client mittels SSH zu verwenden.

- **Telnet**
  Der Telnetdienst von Windows Server 2003 unterstützt in bestimmten Fällen NTLM-Authentisierung (Protokoll für verschlüsselte Authentisierung unter Windows), schaltet standardmäßig jedoch auf Klartextauthentisierung zurück, wenn der Client ein UNIX-Telnet-Client oder ein Windows-basierter Client ist, der nicht NTLM verwendet. Alle weiteren Daten werden immer unverschlüsselt übertragen. Daher sollte Telnet grundsätzlich nur in einem isolierten

Bereich oder über einen sicheren Kanal, beispielsweise mittels SSH, verwendet werden.

- **LPR/LPD**
  Das Druckprotokoll *Line Printer Request/Line Printer Daemon* (LPR/LPD) ist in den Druckdiensten für UNIX enthalten. Es ist ein unsicheres, nicht spezifiziertes Protokoll. Es sollte daher in einer Windows-Umgebung nicht verwendet werden. Ab Windows Server 2003 wird das *Internet Printing Protocol* (IPP) unterstützt, das auch im verbreiteten UNIX-Druckdienst *CUPS* enthalten ist.

- **ARP**
  Für das *Adress Resolution Protocol* (ARP) werden standardmäßig keine Einstellungsmöglichkeiten für die Sicherheit angeboten. Windows Server 2003 verwaltet den ARP-Cache automatisch. Die Sicherheitsanforderungen müssen hier auf Seiten der Netzwerkkomponenten wie Netzwerkverteiler und Sicherheits-Gateways realisiert werden. Bei IT-Systemen mit besonderem Schutzbedarf kann überlegt werden, statische ARP-Einträge für das Standardgateway und für bestimmte kritische Kommunikationspartner zu generieren, z. B. andere Server der lokalen IT-Umgebung. Der Befehl an der Kommandozeile lautet unter Windows XP/2003 (Beispiel):

  ```
  arp –s 192.168.85.212 00-aa-00-62-c6-09
  ```

  Als IP- und Hardware-Adresse müssen die Adressen des gewünschten Kommunikationspartners angegeben werden.

4 Absichern der IIS-Basis-Komponente unter Windows Server 2003

Welche Komponenten können installiert werden?

0. Öffnen von *Start* | *Systemsteuerung* | *Software* | *Windowskomponenten hinzufügen/entfernen.*

0. Unter *Anwendungsserver* sollten nur *COM+-Netzwerkzugriff aktivieren* und *Internetinformationsdienste* (IIS) aktiviert sein.

0. Unter *Internetinformationsdienste* (IIS) dürfen nur *Gemeinsame Dateien*, *Informationsdienste-Manager* und *WWW-Dienst* aktiviert sein; optional darf auch *Internetdrucken* aktiviert werden.

0. Unter *WWW-Dienst* darf nur der Unterpunkt *WWW-Dienst* aktiviert sein; optional darf auch *WebDAV-Veröffentlichung* aktiviert werden. Falls in Punkt 3 *Internetdrucken* aktiviert wurde, dann ist auch *Active Server Pages* aktiv.

0. Falls *Internetdrucken* aktiviert wurde, dann sind *Active Server Pages* folgendermaßen zu verweigern: *Start* | *Systemsteuerung* | *Verwaltung* | *Internetinformationsdienste-Manager* öffnen, auf *Webdiensteerweiterung* klicken und in der Liste die *Active Server Pages* verweigern; die Fehlermeldung bezüglich *Internetdrucken* kann ignoriert werden.

Mit den alternativen Technologien *WebDAV* und *Internetdrucken* können Daten und Drucker über das IP-Netz bereitgestellt werden, ohne das RPC-Protokoll zu verwenden. Neben den genannten Funktionen darf auch die URL-basierte Authentifizierung des IIS 6.0 verwendet werden.

Hinweis: Mit der genannten Konfiguration werden dynamische Inhalte deaktiviert. Die im IIS enthaltene HTML-basierte Remoteverwaltung des Servers und die Remotedesktop-Webverbindung können dann nicht mehr aktiviert werden.

Zugriff einschränken und absichern

Hinweis: Mit den unten genannten Einstellungen wird unter anderem der Netzzugriff auf den lokalen Computer (IP-Adresse 127.0.0.1) eingeschränkt. Andere Computer müssen gezielt nach Bedarf hinzugefügt werden.

Start | *Systemsteuerung* | *Verwaltung* | *Internetinformationsdienste-Manager*

Websites absichern: **Websites**

0. Eigenschaften von *Websites* | Reiter *Verzeichnissicherheit* | *Authentifizierung und Zugriffsteuerung* bearbeiten

0. Option *Anonymen Zugriff aktivieren* deaktivieren, unter *Authentifizierter Zugriff* nur *Integrierte Windows-Authentifizierung* aktivieren, mit *Ok* bestätigen

0. Eigenschaften von *Websites* | Reiter *Verzeichnissicherheit* | *Einschränkungen für IP-Adressen und Domänennamen* bearbeiten

4. *Zugriff verweigert* aktivieren, der Ausnahmeliste die IP-Adresse 127.0.0.1 hinzufügen, mit *OK* bestätigen
5. Einstellungen mit *OK* bestätigen und auf alle untergeordnete Knoten übernehmen
6. Eigenschaften der Standardwebsite | Reiter *Website* | das Feld *IP-Adresse* von *(keine zugewiesen)* auf eine feste IP-Adresse umstellen und ebenso für alle Websites/virtuellen Server verfahren

FTP-Sites absichern:

FTP-Sites

1. Neues lokales Benutzerkonto erstellen, sämtliche Gruppenmitgliedschaften entfernen, Kennwort gemäß den Sicherheitsrichtlinien vergeben, regelmäßige Kennwortänderung gemäß den Sicherheitsrichtlinien beachten
2. Eigenschaften von *FTP-Sites* | Reiter *Sicherheitskonten* | Option *Nur anonyme Verbindungen zulassen* aktivieren
3. Im Feld *Benutzername* den in Punkt 1 angelegten Benutzernamen und das Kennwort eintragen
4. Eigenschaften von *FTP-Sites* | Reiter *Verzeichnissicherheit* | *Zugriff verweigert* aktivieren, der Ausnahmeliste die IP-Adresse 127.0.0.1 hinzufügen
5. Mit *OK* bestätigen, Kennwort bestätigen
6. Eigenschaften der *Standard-FTP-Site* | Reiter *FTP-Site* | das Feld *IP-Adresse* von *(keine zugewiesen)* auf eine feste IP-Adresse umstellen; dasselbe für alle FTP-Sites/virtuellen Server durchführen

Virtuellen Standardserver für NNTP absichern:

Virtueller Standardserver für NNTP

1. Eigenschaften von *Virtuellen Standardserver für NNTP* | Reiter *Zugriff* | *Authentifizierung…*
2. Option *Anonyme Anmeldung erlauben* deaktivieren, nur *Integrierte Windows-Authentifizierung* aktivieren, mit *OK* bestätigen
3. Eigenschaften von *Virtuellen Standardserver für NNTP* | Reiter *Zugriff* | *Verbindung…*
4. *Nur Computer in der Liste* aktivieren, der Liste die IP-Adresse 127.0.0.1 hinzufügen, mit *OK* bestätigen
5. Eigenschaften von *Virtueller Standardserver für NNTP* | Reiter *Allgemein* | das Feld *IP-Adresse* von *(keine zugewiesen)* auf eine feste IP-Adresse umstellen und ebenso für alle virtuellen NNTP-Server verfahren
6. Alle Einstellungen mit *OK* übernehmen

Virtuellen Standardserver für SMTP absichern:

Virtueller Standardserver für SMTP

1. Eigenschaften von *Virtuellen Standardserver für SMTP* | Reiter *Zugriff* | *Authentifizierung…*

2. Option *Anonyme Anmeldung erlauben* deaktivieren, nur *Integrierte Windows-Authentifizierung* aktivieren, mit *OK* bestätigen

0. Eigenschaften von *Virtuellen Standardserver für NNTP* | Reiter *Zugriff* | *Verbindung…*

0. *Nur Computer in der Liste* aktivieren, der Liste die IP-Adresse 127.0.0.1 hinzufügen, mit *OK* bestätigen

0. Eigenschaften von *Virtueller Standardserver für SMTP* | Reiter *Allgemein* | das Feld *IP-Adresse* von *(keine zugewiesen)* auf eine feste IP-Adresse umstellen; dasselbe für alle virtuellen SMTP-Server durchführen

0. Alle Einstellungen mit *OK* übernehmen

Auf allen Virtuellen Servern und Sites sollten grundsätzlich nur die IIS-Rechte *Lesen* und *Besuche protokollieren* gewährt werden. Das Recht *Skriptzugriff* ist besonders gefährlich und darf nur in isolierten Entwicklungsumgebungen verwendet werden. Die weiteren Optionen des Internetinformationsdienste-Managers sind standardmäßig auf eine ausreichende Basissicherheit abgestimmt, welche nicht unnötig aufgeweicht werden sollte.

Verschlüsselung in einem sicherem Kanal (SSL/TLS)

In Verbindung mit einer Organisationszertifizierungsstelle erfolgt die Online-Anforderung und Installation eines Zertifikats assistentengestützt. Die Sicherheitsrisiken beim Transport bzw. der Übertragung sowie beim Einspielen des Zertifikats werden reduziert. Daher empfiehlt sich eine Instanz der Windows-Server-2003-Zertifikatsdienste im lokalen Netz. Der Assistent wird in der Konsole des Internetinformationsdienste-Manager im *Eigenschaften*-Dialogfenster des virtuellen Servers unter *Verzeichnissicherheit* | *Serverzertifikat…* gestartet. Die Verschlüsselung kann dann unter *Verzeichnissicherheit* im Abschnitt *Sichere Kommunikation* | *Bearbeiten…* aktiviert werden. Dazu sind die Optionen *Sicheren Kanal voraussetzen (SSL)* und *128-Bit-Verschlüsselung erforderlich* zu aktivieren.

Hinweis: Die Zertifizierungsdienste sollten aufgrund ihrer strategischen Bedeutung für die Sicherheit der gesamten IT-Umgebung nicht leichtfertig installiert werden. Sie erfordern eine fundierte Planung und sorgfältige Umsetzung (Siehe Hilfsmittel zum IT-Grundschutz, *Schutz der Zertifikatsdienste unter Windows Server 2003*)

Web-Dienste sind plattformunabhängig und können potentiell über die Grenzen der plattformgebundenen Sicherheitsinfrastruktur von Windows Server 2003 (Authentisierung, abgesicherte Netzverbindungen, Sicherheits-Gateways) hinweg eingesetzt werden. Daher sollte in einer Sicherheitsrichtlinie zur Administration von IT-Systemen festgelegt werden, welche administrativen und infrastrukturellen Dienste verschlüsselt werden müssen. Eine SSL-Verschlüsselung für alle Web-basierten administrativen und infrastrukturellen Dienste auf einem Windows-Server-2003-System ist in jedem Fall zu empfehlen. Dies sollte auch organisatorisch in einer entsprechenden Richtlinie festgelegt werden.

Isolieren von Anwendungsprozessen für dynamische Inhalte

ASP-Anwendungen werden standardmäßig von Prozessen des Anwendungspools *DefaultAppPool* ausgeführt. Dieser kann wie folgt deaktiviert werden:

Start | *Systemsteuerung* | *Verwaltung* | *Internetinformationsdienste-Manager* | *Anwendungspools* | auf *DefaultAppPool* klicken | Menüpunkt *Aktion* | *Beenden*

Es ist zu empfehlen, den Anwendungspool *DefaultAppPool* grundsätzlich deaktiviert zu lassen und ASP-Anwendungen in eigenen Prozessen bzw. Anwendungspools zu isolieren.

Standardmäßig wird in einem neu erstellten Anwendungspool maximal ein Prozess gleichzeitig ausgeführt. Dieser läuft mit den eingeschränkten Berechtigungen des vordefinierten Systemkontos *Netzwerkdienst*. Die Standardeinstellungen sollten nicht verändert werden. Gegebenenfalls erforderliche administrative Berechtigungen kann der Benutzer durch seine Anmeldung mit Administratorrechten gewähren.

5 Nutzung von Sicherheitsvorlagen unter Windows Server 2003

Die wichtigsten Werkzeuge für Sicherheitsvorlagen sind:

Sicherheitskonfigurationseditor (SCE)

- Berechtigungen in Registrierdatenbank und Dateisystem setzen
- Systemrechte einstellen
- Startverhalten von Diensten festlegen
- Überwachungseinstellungen konfigurieren
- Basis-Sicherheitsoptionen für das Systemverhalten, Netzwerkverkehr und Benutzerkonten konfigurieren
- Sicherheitsvorlagendateien des SCE haben die Erweiterung *.inf*

Sicherheitskonfigurations-Assistent (SCW, erst ab Service Pack 1 enthalten)

- identifiziert offene Ports (der Assistent sollte erst aufgerufen werden, wenn alle benötigten Anwendungen und Dienste aktiv sind)
- Auswahl von Rollen aus einem Konfigurations-Katalog
- konfiguriert die benötigten Dienste
- konfiguriert spezifische Einstellungen für die jeweiligen Serverrollen
- konfiguriert Ports für die Windows-Firewall
- konfiguriert LDAP- und SMB-Sicherheit
- konfiguriert eine Überwachungsrichtlinie
- kann einige Einstellungen der Internetinformationsdienste konfigurieren
- Sicherheitsvorlagen des SCW werden in XML-Dateien gespeichert
- als Grundlage für IT-Dokumentation geeignet

SCEregvl.inf aktualisieren

Sicherheitsoptionen im SCE sichtbar machen

In der Herstellerdokumentation "*Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*" Version 2.0 vom 27. Dezember 2005 sind Einstellungen, die auf Windows Server 2003 mit Service Pack 1 abgestimmt sind, enthalten. Es ist zu empfehlen, die Einstellungen auf dem Server in den SCE-Konsolen sichtbar zu machen. Die zentrale Konfigurationsdatei hierfür bildet *C:\WINDOWS\inf\SCEregvl.inf*. Ansonsten müssen einige Einstellungen aus den Windows-Server-2003-Maßnahmen des IT-Grundschutzhandbuches manuell in die Registrierdatenbank geschrieben bzw. als administrative Vorlage implementiert werden.

Hinweise zur Einbindung der Einstellungen in den SCE:

- die Dateien *Values-sceregvl.txt*, *Strings-sceregvl.txt* und *Update_SCE_with_MSS_Regkeys.vbs* aus der Anlage der o. g. Herstellerdokumentation in einen neuen Ordner kopieren
- *Update_SCE_with_MSS_Regkeys.vbs* ausführen, Meldungen mit *OK* bestätigen

Hinweise zur manuellen Einbindung befinden sich auch in der Herstellerdokumentation. Die Einbindung funktioniert nicht nachträglich auf einem Mitgliedsserver oder Domänencontroller.

Einige der Einstellungen werden automatisch vom *Sicherheitskonfigurations-Assistenten* (SCW) gesetzt, wenn eine Serverrolle dies erfordert. Dies wird über die hinzugefügten SCE-Einstellungen sichtbar.

Herstellerunterlagen auf Aktualisierungen prüfen

Es ist zu prüfen, ob die Herstellerdokumentation in einer aktuelleren Version vorliegt. Es sollten die jeweils neusten Sicherheitsoptionen für den SCE berücksichtigt werden.

Sicherheitskonfigurations-Assistent (SCW)

SCW-basierte Sicherheitsrichtlinien sind keine Richtlinien im Sinne des Grundschutz

Der SCW analysiert und konfiguriert das System auf Grundlage der Empfehlungen des Herstellers für bestimmte Serverrollen bzw. speichert die empfohlenen Einstellungen in XML-Richtliniendateien ab. Die Empfehlungen sind in den Dokumentationsunterlagen des Herstellers *Windows Server 2003 Security Guide* und *Threats and Countermeasures*, jeweils vom 27. Dezember 2005 oder aktueller zu finden. Die im SCW verwendete Bezeichnung *Sicherheitsrichtlinie* ist nicht im Sinne von Sicherheitsrichtlinien nach Grundschutz zu verstehen.

Der Assistent durchläuft die fünf Abschnitte

- Rollenbasierte Konfiguration
- Netzwerksicherheit
- Registrierungseinstellungen
- Überwachungsrichtlinie
- Internetinformationsdienste

SCW-Vorlagen müssen ergänzt werden

Dort werden Anhaltspunkte für sinnvolle Sicherheitseinstellungen und für das Schreiben eigener Betriebsrichtlinien geliefert. In den meisten Szenarien ist der Satz vorgegebener Einstellungen jedoch nicht ausreichend, um die Maßnahmen für den normalen Schutzbedarf oder die vorhandenen IT-Sicherheitsrichtlinien umzusetzen. Für das Bereitstellen einer sicheren Basiskonfiguration von Windows Server 2003 ist weiterer Aufwand erforderlich. Daher ist im Einzelfall der Gesamtaufwand gegen den Nutzen von SCW-basierten Vorlagen abzuwägen.

Kombination von SCE und SCW

An eine SCW-basierte Vorlage können Sicherheitsvorlagen des SCE angehängt werden. Falls dadurch Einstellungen doppelt definiert sind, dominieren die Einstellungen des SCW. Die Abschnitte *Registrierungseinstellungen* und *Überwachungsrichtlinie* sollten daher ganz ausgeklammert und hierfür eigene SCE-Sicherheitsvorlagen erstellt werden. Bei den anderen Abschnitten ist im Einzelfall zu prüfen, welcher Vorlagentyp besser geeignet ist. Für höhere Flexibilität bei den Einstellungen und bei der Ausrollstrategie sind Sicherheitsvorlagen des SCE besser geeignet.

Automatische Rollback-Vorlage

Beim Anwenden einer SCW-Sicherheitsrichtlinie wird automatisch eine Rollback-Vorlage generiert und im Verzeichnis *C:\WINDOWS\security\msscw\RollbackFiles* gespeichert. Darauf basierend bietet der Assistent ein so genanntes Sicherheitsrichtlinienrollback an. Hier gelten die gleichen Einschränkungen wie beim Rollback von Sicherheitsvorlagen des SCE. Dies kann insbesondere im Abschnitt *Überwachungsrichtlinie* – in diesem Abschnitt werden Objekt-Überwachungseinstellungen (SACL) konfiguriert – und bei angehängten Sicherheitsvorlagen leicht zu Komplikationen führen. Daher sollten für

rollbackkritische Einstellungen Sicherheitsvorlagen unabhängig vom SCW erstellt werden.

Manuelle Anpassungen der Assistent-Vorgaben

Zur Erhöhung der Sicherheit sind besonders die Abschnitte *Rollenbasierte Konfiguration*, *Internetinformationsdienste* und *Netzwerksicherheit* geeignet. Die Einstellungen unter *Rollenbasierte Konfiguration* sollten gemäß den jeweiligen Grundschutzmaßnahmen und IT-Sicherheitsrichtlinien angepasst werden. Die Internetinformationsdienste sollten über die SCW-Einstellungen hinaus mit anderen Mitteln weiter abgesichert werden (M 4.282 *Sichere Konfiguration der IIS-Basiskomponente unter Windows Server 2003*).

SCW-Vorlagen für Windows-Firewall erhöhen die Gesamtsicherheit

Der Abschnitt *Netzwerksicherheit* ist gut zur Konfiguration der Windows-Firewall für normale Anforderungen geeignet, da meist keine manuellen Anpassungen mehr nötig sind. Sofern keine ungetesteten Serverapplikationen von Drittherstellern auf den Servern installiert sind, kann mittels SCW-Vorlage und aktivierter Windows-Firewall die Sicherheit für einen Bereich von Servern mit geringem Entwicklungs- und Testaufwand erhöht werden (Näheres siehe M 4.280 *Sichere Basiskonfiguration von Windows Server 2003*).

SCW-Vorlagendateien sollten nicht nach Computernamen benannt werden, auf denen sie angewendet werden, da automatische Rollbackdateien und Protokolldateien nach dem Muster *%Computername%.xml* generiert werden und die Gefahr von Verwechselungen oder versehentlichem Löschen besteht.

Für SCW-Vorlagen sollten die gleichen Konformitätsanforderungen gelten wie für SCE-Sicherheitsvorlagen. Außerdem sollte auch hier der Katalog mit den verfügbaren Optionen (unter *C:\WINDOWS\security\msscw\kbs*) aktualisiert werden, sobald eine aktuellere Version vom Hersteller verfügbar ist.

6 Planung der Windows 2000/2003 CA-Struktur

Strukturelle Planungsaspekte

- Soll eine eigene Wurzel-CA (Root-CA) betrieben werden? Wird keine eigene Wurzel-CA betrieben, muss entschieden werden, welche externe CA als Wurzel-CA akzeptiert wird. Generell können zwar auch mehrere externe CAs als Wurzel-CA akzeptiert werden, dies sollte jedoch aus Gründen der Einheitlichkeit der intern verwendeten Zertifikate vermieden werden (ein Zertifikat hat immer nur eine Wurzel-CA).
- Welche CA ist welcher anderen CA untergeordnet?
- Ist eine Vertrauenstellung zu einer anderen PKI erforderlich (mittels *qualifizierte Unterordnung*, ab Windows Server 2003)?
- Welche CA stellt welche Zertifikatstypen in Abhängigkeit vom Verwendungszweck aus?
- Auf welche Namensbereiche und Fähigkeiten sollen untergeordnete CA's eingeschränkt werden (*Namenseinschränkung* und *Richtlinieneinschränkung* von Zertifikaten, ab Windows Server 2003)?
- Nach welchen Kriterien wird bei einer Zertifikatsanfrage positiv entschieden? Ist z. B. eine Überprüfung von Personalien notwendig?
- Welche Benutzer und Rechner dürfen auf eine CA zugreifen?
- Werden Zertifikatsrückruflisten benötigt, und wo und wie werden diese veröffentlicht?
- Auf welchen Rechnern werden welche PKI-Komponenten installiert? Wo laufen die CA-Komponenten ab?

Planung des Einsatzes geeigneter Zertifizierungsstellen

- In vielen Ländern unterliegen elektronische Zertifikate einer gesetzlichen Regelung. Die geltenden Gesetze sind daher bei der Planung zu berücksichtigen. Beispiele sind Schlüssellänge und verwendete Algorithmen. Dabei muss beachtet werden, dass bei weltweit agierenden Organisationen auch mehrere Gesetzesvorschriften gelten können, die durchaus auch im Widerspruch zueinander stehen können (siehe auch M 2.163 *Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte*). Die gesetzlichen Regeln gelten für betriebsinterne PKIs nur eingeschränkt.
- Es ist weiterhin zu beachten, dass Zertifikate trotz (bzw. wegen) einer Vielzahl von Normen in der Regel nicht automatisch universell mit allen Applikationen eingesetzt werden können. Die fehlende Interoperabilität resultiert aus mehreren Ursachen. Dazu gehören neben tatsächlichen Normverletzungen bei der Implementierung außerdem die Interpretationsspielräume, die in den Spezifikationen der verschiedenen Normen existieren.

- Der Einsatz der Microsoft Enterprise-CA ist vorteilhaft, wenn Smartcard-basiertes Logon eingesetzt werden soll oder wenn SSL zur Absicherung der Kommunikation zwischen Windows-Systemkomponenten, z. B. beim LDAP-Zugriff, genutzt werden soll. Dies ist notwendig, da in beiden Fällen Rechnerzertifikate erforderlich sind, die nur von der Enterprise-CA automatisch in größerem Umfang vergeben werden können.

7 Administration der Berechtigungen unter Windows Server 2003

Erläuterungen zu Berechtigungseinstellungen in bestimmten Bereichen von Windows Server 2003

Benutzer-unabhängige Berechtigungen

Bei den Internet Information Services (IIS) gibt es zusätzliche, rein ressourcenbasierte Berechtigungsmechanismen, die pauschal auf die Ressource gesetzt werden und unabhängig von einer Konto-Authentisierung für jeden Zugriff gelten. Dieselben Ressourcen haben ergänzend dazu auch authentisierungsgebundene Zugriffsberechtigungen. Ebenfalls in den IIS sowie in darauf aufbauenden Komponenten wie *Anwendungsserver* steht die URL-basierte Zugriffskontrolle zur Verfügung. Die Zugriffsberechtigungen werden in einem separaten *Autorisierungsrichtlinienspeicher* der IIS-*Metabase* hinterlegt und können z. B. durch Skripte administriert werden.

Systemrechte (engl. rights/privileges)

Weiterhin können durch Gruppenrichtlinien Einschränkungen und Rechte festgelegt werden, die den Zugriff auf Betriebssystemfunktionen und Funktionen von Applikationen steuern. Mit Gruppenrichtlinien in Zusammenhang mit Active Directory und authentisierungsgebundenen Zugriffsberechtigungen können die wirksamen Berechtigungen sehr fein granuliert werden.

Rollenbasiertes Zugriffsmanagement

In der Konsole *Autorisierungs-Manager* kann ein rollenbasiertes Zugriffsmanagement (*Role Based Access Control*, RBAC) realisiert werden. Der Entwurf von Rollen setzt zunächst eine rein organisatorische Betrachtungsweise voraus und orientiert sich an definierbaren Arbeitsprozessen und der personellen Organisation. Das organisatorische Modell wird dann in ein Autorisierungsmodell für Windows Server 2003 abstrahiert, welches Funktionsdefinitionen, Rollenzuweisungen Aufgaben-definitionen, Vorgangsdefinitionen umfasst. Einem Benutzerkonto können Funktionen und Rollen zugeordnet werden. Aufgabendefinitionen und Vorgangsdefinitionen enthalten letztlich skript-basierte Autorisierungsregeln, welche die erforderlichen Berechtigungen in den beteiligten IT-Systemen setzen und Ressourcen bereitstellen. Skripte für Autorisierungsregeln müssen in den meisten Fällen selbst erstellt werden, da nur wenige Anwendungen eine Unterstützung für RBAC mitbringen. RBAC ist somit ein aufwendiger und kostenintensiver Ansatz, um die Administration von Berechtigungen in größeren Umgebungen zu automatisieren und effektiver zu strukturieren. Die Sicherheit des betrachteten IT-Verbundes kann aufgrund der organisatorischen Verbesserungen erhöht werden. Allerdings erhöht der systemübergreifende Ansatz von RBAC die Risiken durch unzureichende Planung sowie durch die Zahl von beteiligten Systemkomponenten und deren unsachgemäßer Bedienung.

Hinweise zu Strategien der Berechtigungsvergabe

Explizites verweigern von Berechtigungen vermeiden

Das Verweigern von Zugriffsrechten auf ein Objekt dominiert immer über alle anderen Rechtezuweisungen. Die unmittelbaren und mittelbaren Auswirkungen von expliziten Verweigerungen können nur durch eine sorgfältige Konzeption und Dokumentation von Berechtigungen vorausgesehen werden. Die Verweigerungen sollten folglich nur sehr gezielt

verwendet und explizit in der Dokumentation vermerkt werden. Verweigerungen im laufenden Betrieb können sehr riskant für die Systemverfügbarkeit sein und sollten vermieden werden. Vor dem Setzen von Verweigerungen sollte dies mit den jeweiligen Fachverantwortlichen abgestimmt werden.

Systemberechtigungen nicht manipulieren

Vorhandene Systemberechtigungen und Vererbungseinstellungen von Systemobjekten sollten grundsätzlich nicht verändert werden, da das System so in einen nicht administrierbaren und gegebenenfalls nicht mehr betriebsfähigen Zustand geraten kann. Generell sollten Änderungen von Vererbungseinstellungen auch bei Benutzerdaten am Ende einer Vererbungskette begonnen und getestet werden. Bei der unüberlegten Aktivierung oder Deaktivierung der Vererbung auf einem übergeordneten Objekt besteht die Gefahr, dass wichtige Zugriffsberechtigungen der darunter liegenden Struktur zurückgesetzt werden. Spezielle Berechtigungsstrukturen, z. B. für delegierte Administratoren, gehen verloren. Berechtigungskonzepte sollten so ausgelegt sein, dass Änderungen von Zugriffsberechtigungen an Objekten im Normalbetrieb nicht oder nur in Ausnahmefällen notwendig sind.

Vererbung innerhalb großer Strukturen

Ressourcen-berechtigungen vorrangig an Gruppen vergeben

Aus den oben genannten Gründen empfiehlt es sich bei der Vergabe von Zugriffsrechten auf Objekte immer, Sicherheitsgruppen den Vorzug vor einzelnen Benutzerkonten zu geben. Benutzerkonten erhalten die Berechtigungen, indem sie der Gruppe hinzugefügt werden. Nur bei hohen Vertraulichkeitsanforderungen (z. B. für ein privates Benutzerverzeichnis) oder sehr sicherheitskritischen Systemkomponenten (z. B. Zertifizierungs-dienste) werden direkt Benutzerkonten oder administrative Konten angegeben. In solchen Fällen sollte das Verfahren klar in einem eigenen Konzept für die jeweilige Anforderung definiert sein.

Verzögerte Wirkung von Berechtigungs-änderungen

Zugriffsberechtigungen auf Objekte wirken sofort, nachdem sie gesetzt wurden, d. h. angemeldete Benutzer können die resultierenden Rechte unmittelbar ausüben. Rechte, die aus Änderung der Gruppenmitgliedschaft eines Kontos entstehen, können erst nach Erhalt eines neuen Kerberos-Tickets ausgeübt werden. Dies geschieht in den meisten Fällen durch einen erneuten Authentisierungsvorgang (indem Benutzer sich abmelden und erneut anmelden). Bei der Verwendung von Active Directory sind Sicherheitsgruppen oft Mitglieder in anderen Gruppen, woraus sich für Benutzerkonten eine indirekte Mitgliedschaft in anderen Gruppen ergibt. Auch wenn sich die indirekte Mitgliedschaft ändert, kann das Benutzerkonto die resultierenden Rechte erst nach einer Neuanmeldung ausüben. Durch diesen Effekt können Auswirkungen von Konfigurationsänderungen über einen längeren Zeitraum unbemerkt bleiben oder unter Umständen nicht korrekt evaluiert werden, z. B. wenn Benutzer längere Zeit an ihrem Client angemeldet bleiben, wenn Applikationsprozesse während der Abarbeitung einer Aufgabe längere Zeit in einem bestimmten Sicherheitskontext laufen oder letztlich bei Windows-Diensten, die auf Servern üblicherweise permanent aktiv sind. Teil jeder Konfigurationsänderung im laufenden Betrieb sollte also immer das Ab- und Anmelden von betroffenen Konten sein. Dafür muss gegebenenfalls ein Wartungsfenster eingeplant werden. Voraussetzung für eine sichere Administration ist auch hier die sorgfältige Dokumentation der Konten und Berechtigungen.

8 Bereitstellungskonzept von Windows Server 2003

Für das Bereitstellungskonzept zu berücksichtigende Aspekte

In einem Bereitstellungskonzept kommen übergreifende Aspekte hinzu, unter anderem:

- Bereitstellungsstrategie: Setup-Programm oder Festplattenabbild (siehe oben), Installationsquelle online im Netz oder offline auf Installationsmedium
- isolierter Netzbereich für die Installation
- Auswahl geeigneter Lizenzprogramme des Herstellers, z. B. Volumenlizenzen
- Erstellen von Antwortdateien (*unattended.txt*, *winnt.sif*, *winpeoem.sif*)
- Schutz des Produktschlüssels in Antwortdateien
- Installationsquellen anpassen (Treiber integrieren, weitere Softwarekomponenten bereitstellen)
- Schutz der angepassten Installationsmedien oder -quellen
- Automatische Produktaktualisierung
- Erstellen von Post-Installationsskripten
- Bereitstellung von Konfigurationsvorlagen, z. B. per Skript oder Gruppenrichtlinien
- Auswahl geeigneter Standardsoftware für die Verteilung von Software oder für die Erstellung und Verteilung von Festplattenabbildern
- SID ändern (bei Festplattenabbild)
- Remote-Boot-Umgebung, besonderer Schutz der Kommunikationsprotokolle für Remote-Boot (z. B. isoliertes Installationsnetz)
- Einsatz eines Installationsservers
- Zusammenspiel mit anderen Konzepten (Administration, Wiederherstellung, Notfallplanung, Active Directory, IT-Änderungs-management)

Produktschlüssel verschlüsseln

Produktschlüssel und Kennwörter in Antwortdateien sind besonders schützenswert. Ab Windows Server 2003 mit Service Pack 1 kann der Produktschlüssel mit Hilfe des Programms *Winnt32.exe* (Verzeichnis *\i386* auf der Installations-CD bzw. CD1 bei Windows Server 2003 R2) verschlüsselt werden:

Aufruf an der Kommandozeile:

```
winnt32.exe /encrypt:"xxxxx-xxxxx-xxxxx-xxxxx-
xxxxx:y" /unattend:unattended.txt
```

Die *x*-Buchstaben stehen für den Produktschlüssel, *y* ist die Gültigkeitsdauer der Chiffre in Tagen (max. 60 Tage, danach muss der Befehl erneut ausgeführt werden). Anstelle von *unattended.txt* können auch andere Antwortdateien verwendet werden.

Installationskennwörter schützen

Kennwörter werden zwecks Domänenbeitritts, zum Ausführen von Post-Installationsskripten sowie zum Setzen des lokalen Administrator-Kontos in die Antwortdatei eingetragen. Kennwörter aus der produktiven Umgebung

dürfen nicht im Klartext gespeichert oder übertragen werden. Für das lokale Administrator-Kennwort sollte im Setup-Manager unter *Network Settings* | *Administrator Password* die Option *Encrypt the Administrator Password in the answer file* aktiviert werden. Dadurch wird auch die Funktion *Autologon* für den lokalen Administrator verhindert (*Autologon* speichert das Klartext-Kennwort in der Windows-Registrierung). Sonstige Kennwörter können nicht verschlüsselt werden. Daher dürfen Kennwörter aus der produktiven Umgebung weder in Antwortdateien noch Post-Installationsskripten verwendet werden. Sind unverschlüsselte Kennwörter aus organisatorischen Gründen nicht zu vermeiden, muss der Server während der Installation vor unberechtigtem Zugang geschützt und netzseitig isoliert werden.

Geschützte Produktaktivierung

Die Online-Produktaktivierung benötigt eine aktive Internetverbindung und das HTTP-Protokoll. Während der Installationsphase sollte die Aktivierung nur über ein Sicherheits-Gateway mit Proxyserver durchgeführt werden, d. h. in der Antwortdatei darf die Option *AutoActivate* ausschließlich gemeinsam mit der Option *ActivateProxy* verwendet werden. Dazu muss die Antwortdatei manuell editiert werden. Die Aktivierung kann auch später skriptgesteuert (z. B. im Post-Installationsskript) oder manuell ausgelöst werden. Die meisten Lizenzen erlauben einen Zeitraum von 30 Tagen ohne Aktivierung. So werden auch überflüssige Aktivierungen für fehlgeschlagene oder verworfene Installationen vermieden. Bei hohem Schutzbedarf des Servers kann auf die telefonische Aktivierung ausgewichen werden.

Hinweis: Die Herstellerdokumentation zum Thema Antwortdateien ist in den Dateien *ref.chm* und *deploy.chm* auf der Installations-CD bzw. CD1 bei Windows Server 2003 R2 in *\SUPPORT\TOOLS\DEPLOY.CAB* zu finden.

9 Schutz der Zertifikatsdienste unter Windows Server 2003

PKI

Zertifikatsdienste sind Teil einer umfangreichen, systemübergreifenden Struktur, der so genannten *Public Key Infrastructure* (PKI). Bevor die Maßnahme angewendet werden kann, sollten unter Berücksichtigung des Kryptokonzeptes der Einsatzzweck der Zertifikatsdienste und die Strategie für eine PKI festgelegt werden. Vorrausetzungen für den sicheren und effektiven Einsatz der Zertifizierungsdienste sind:

- Schulung der Administratoren in der Windows-Implementation der Zertifizierungsstellen und Active Directory
- PKI-Konzept (siehe M 2.232 *Planung der Windows 2000/2003 CA-Struktur*)
- Prüfung, ob einschichtige oder mehrschichtige PKIs und/oder Kreuzzertifizierung (so genannte *qualifizierte Unterordnung*) zum Einsatz kommen
- Prüfung, ob der Einsatz von Active Directory möglich bzw. geplant ist (gegebenenfalls M 2.229 *Planung des Active Directory* umsetzen)
- Festlegung der Applikationen und Infrastrukturdienste, in denen Zertifikate benutzt werden sollen

Diese Maßnahme befriedigt nicht den besonderen Schutzbedarf für Zertifikatsdienste von Zertifizierungsdiensteanbietern gemäß Signaturgesetz (SigG) und Signaturverordnung (SigV).

Absicherungsbedarf von Zertifizierungsstellen

Einsatzbereich und Einsatzzweck der einzelnen Zertifizierungsstelle beeinflussen stark ihren jeweiligen Absicherungsbedarf und den dafür zu leistenden Aufwand. Beispielsweise kann die Stammzertifizierungsstelle (auch Wurzel- oder Root-CA genannt) in einer mehrschichtigen PKI-Hierarchie einen sehr hohen Schutzbedarf haben. Unter Umständen ist die Sicherheit der PKI bzw. einer Zertifizierungsstelle der limitierende Faktor für die Gesamtsicherheit einer zertifikatsbasierten Anwendung oder Komponente. Der notwendige Absicherungsbedarf sollte für jede Zertifizierungsstelle geklärt sein.

Die meisten Windows-Komponenten, die Zertifikatsdienste verwenden, bevorzugen bzw. benötigen eine Active-Directory-integrierte Zertifizierungstelle. Unter Windows Server 2003 spielen Zertifikatsdienste in verschiedenen Bereichen eine Rolle, z. B.

- *Internet Information Services* (IIS)
- IPSec
- *Encrypting File System* (EFS)
- Benutzeranmeldung, z. B. mit Smartcards
- Clientauthentisierung, z. B. für verschlüsselte Authentisierungsmethoden bei IEEE 802.1x und anderen Protokollen.

Eigenständige Zertifizierungsstellen

Die Installation von eigenständigen, nicht in das Active Directory integrierten Zertifizierungsstellen (auch Stand-Alone-CA genannt) ist in den meisten

Fällen ungeeignet und sollte genau überlegt werden. Besondere Gründe für eine eigenständige CA könnten sein:

- Offlinezertifizierungsstelle
- heterogene oder aus mehreren Gesamtstrukturen bestehende Umgebung in Kombination mit der Zertfizierungsstellenlösung eines Drittanbieters
- exponierter Bereich, in dem ein starkes Sicherheits- und Genehmigungsmodell erforderlich ist

Die Entscheidung zwischen eigenständiger und Active-Directory-integrierter Zertifizierungsstelle wird jedoch auch von Faktoren beeinflusst, die sich aus dem Einsatzbereich und dem Design der PKI ergeben.

Im Folgenden werden Hinweise für die Absicherung einer Zertifizierungsstelle und für umgebungsrelevante Mechanismen der Zertifizierungsdienste gegeben:

- Die Zertifikatsdienste sind grundsätzlich nicht auf einem Domänencontroller zu installieren. In den meisten Fällen empfiehlt es sich, Zertifizierungsstellen auf einem separaten System zu installieren, da andere Dienste durch die Vorkehrungen zur Absicherung der Zertifizierungsdienste auf diesem Server möglicherweise nicht mehr lauffähig sind.
- Auf Zertifizierungsstellen mit hohem Schutzbedarf sollten keine weiteren Dienste und Rollen konfiguriert werden, die Internet Information Services (IIS) eingeschlossen.
- Es ist zu überlegen, die *Web Enrollment Pages* (IIS-basierte Konsolen der Zertifikatsdienste) auf einen oder mehrere separate Server auszulagern, die keine Zertifikatsdienste ausführen. Dadurch wird IIS auf Zertifizierungsstellen vermieden und die Sicherheit der PKI erhöht.
- Zertifikate für untergeordnete Zertifizierungsstellen laufen standardmäßig nach einem Jahr ab. Es ist für eine rechtzeitige Verlängerung zu sorgen. Es ist für sämtliche Zertifikate eine Vorgehensweise festzulegen, wie Zertifikate rechtzeitig erneuert werden. Für Server kann dies z. B. im Rahmen von Wartungsmaßnahmen sichergestellt werden. Die Verlängerung ist ebenfalls mittels *Auto-Enrollment* möglich (siehe M 2.232 *Planung der Windows 2000/2003 CA-Struktur*).
- Es ist sicherzustellen, dass nur die beabsichtigten und geplanten Zertifikatstypen von der einzelnen Zertifikatsstelle ausgestellt werden. Standardmäßig voreingestellte Typen sollten entfernt und nur bei Bedarf wieder hinzugefügt werden. (*Start* | *Systemsteuerung* | *Verwaltung* | *Zertifizierungsstelle* | Eigenschaften der Zertifizierungsstelle | *Zertifikatsvorlagen*). Dies verhindert unbeabsichtigtes Ausstellen von Zertifikaten, z. B. durch *Auto-Enrollment*.

***Hardware Security Module* (HSM)**

Hardware Security Module

Die Sicherheit des Schlüsselpaares (siehe B 1.7 *Kryptokonzept*) einer Zertifizierungsstelle kann durch ein *Hardware Security Module* (HSM) erhöht

werden. HSM dient dem Erzeugen und Aufbewahren des Zertifizierungsstellenschlüsselpaares außerhalb der Zertifizierungsstelle. Mit einem HSM lässt sich die Kontrolle über den privaten Schlüssel der Zertifizierungsstelle auf mehrere Personen verteilen und mindestens ein Vier-Augen-Prinzip realisieren. Die Sicherheit gegen Kompromittierung der Zertifizierungsstelle wird dadurch deutlich erhöht und ist für sehr hohen Schutzbedarf zu empfehlen, z. B. bei Stammzertifizierungsstellen.

Zertifizierungsstelle offline schalten

Trennung der CA vom Netzwerk und Aufbewahrung

Offlinezertifizierungsstellen sind vom Netzwerk zu trennen und an Plätzen mit gesicherter Zugangskontrolle wie z. B. Tresoren aufzubewahren. Dazu muss der Computer abgeschaltet werden. Er wird nur aktiviert, um aktualisierte Zertifikatssperrlisten (*Certificate Revocation List*, CRL) zu veröffentlichen oder um neue Zertifizierungsstellenzertifikate auszustellen. Durch eine sichere Verwahrung bietet eine Offlinezertifizierungsstelle ausreichenden Schutz der Zertifizierungsstellenschlüssel. Mit der Offlinezertifizierungsstelle besteht die Möglichkeit, Zertifikate zu sperren, die von einer kompromittierten untergeordneten Zertifizierungsstelle ausgestellt wurden. Alleinstehende Server mit einer eigenständigen Zertifizierungsstelle sind als Offlinezertifizierungsstelle am besten geeignet.

Sicherung in virtueller Umgebung auf Wechseldatenträger

Wenn kein HSM eingesetzt wird, sollte überlegt werden, eine mindestens zweistufige Hierarchie umzusetzen. Die Stammzertifizierungsstelle sollte dann offline geschaltet und durch organisatorische Maßnahmen geschützt werden.

Für die Offlinezertifizierungsstelle kann Virtualisierungstechnologie eingesetzt werden. Das gesamte Betriebssystem mit den Zertifikatsdiensten wird dann in einer simulierten Hardware-Umgebung installiert. Die virtuelle Umgebung kann leicht auf einem Wechseldatenträger gespeichert und sicher verwahrt werden.

Kennwortschutz Zertifikatsperrliste

Bei einer Offlinezertifizierungsstelle ist es erforderlich, alternative Speicherorte festzulegen, von denen Sperrlisten abgerufen werden können, während die Zertifizierungsstelle offline ist. Es sollte eine Strategie definiert werden, wie eine Sperrliste nach einer Sperrlistenaktualisierung an solche Speicherorte übertragen wird (Veröffentlichung der Sperrliste).

Eine Strategie hierfür kann die Angabe einer UNC-Adresse (*Universal Naming Convention*) als Speicherort sein. Zum Angeben der Adresse, d. h. des Pfades zu einer Zertifikatsperrliste, stehen alle notwendigen Variablen in der Verwaltungskonsole der Zertifizierungsstelle unter *Eigenschaften* | *Erweiterungen* zur Verfügung. Eine UNC-Adresse beginnt hier mit *file://*. Die weiteren Einstellungen in diesem Dialogfenster legen fest, ob die Adresse nur zur Veröffentlichung genutzt wird oder ob sie auch in neu ausgestellten Zertifikaten als Suchpfad für Sperrlisten (*CRL Distribution Point*, CDP) hinterlegt wird. Gültige CDPs werden normalerweise bei der PKI-Planung festgelegt.

In größeren IT-Verbundsystemen kann ein benutzerdefiniertes Beendigungsmodul oder Skript verwendet werden, mit dem die Zertifikatsperrliste an einer vordefinierten Position veröffentlicht wird. Alle erforderlichen Informationen zur Erstellung eines Beendigungsmoduls sind im

Security Platform SDK dokumentiert. Für ein Skript zur Veröffentlichung der Zertifikatssperrliste ist der Kommandozeilenbefehl `certutil –crl` geeignet.

Startkennwort für das Betriebssystem der Offlinezertifizierungsstelle

Alternativ oder zusätzlich zur externen Zugangskontrolle kann das Betriebssystem der Offlinezertifizierungsstelle mit einem Windows-Startkennwort versehen werden, wodurch die Sicherheit weiter erhöht wird. An der Eingabeaufforderung muss dafür das Systemschlüsseldienstprogramm (*Syskey*) durch die Eingabe von `syskey.exe` gestartet werden. Im daraufhin erscheinenden Dialogfenster ist *Aktualisieren* | *Kennwort für den Systemstart* zu klicken, ein mindestens zwölf Zeichen langes komplexes Kennwort zu vergeben und der Vorgang mit *OK* abzuschließen. Das Programm *Syskey* bietet noch weitere Schutzstufen. Der falsche Gebrauch kann jedoch das System für immer sperren und unbrauchbar machen. Der Einsatz von *Syskey* sollte daher vorher in einer Testumgebung erprobt werden.

Sicherung der Stammzertifizierungsstelle

Separate Sicherungsmedien nutzen

Der Verlust der Stammzertifizierungsstelle durch Hardware-Defekte zieht erheblichen organisatorischen Aufwand nach sich. Der Server mit der Zertifizierungsstelle sollte auf einem separaten, geschützten Medium gesichert werden. Dies kann z. B. durch die Sicherung des Systemstatus mit *NtBackup* oder durch das Duplizieren der virtuellen Hardware-Umgebung umgesetzt werden. Die Sicherungsmedien enthalten den privaten Schlüssel und müssen geschützt aufbewahrt werden.

Die Stammzertifizierungsstelle sollte nicht zusammen mit den IIS auf demselben Computer installiert werden.

CAPolicy.inf

Wenn die Zertifizierungsstelle neu aufgesetzt wird, sollte die Konfiguration mittels der Konfigurationsdatei *CAPolicy.inf* vordefiniert werden. Hier werden grundlegende Eigenschaften und Datenfelder der PKI und der ausgestellten Zertifikate festgelegt, unter anderem das Feld für *Certificate Practise Statement* (CPS). Vor dem Installieren der Zertifikatsdienste muss diese Datei in das Standardverzeichnis *C:\WINDOWS* kopiert werden. Die Datei gilt für die gesamte Lebensdauer der Zertifizierungsstelle und ist durch Sicherung und Zugriffsberechtigungen vor Verlust und unberechtigtem Zugriff zu schützen.

Außerdem ist zu überlegen, auf der Stammzertifizierungsstelle nur einen "leeren" CDP zu definieren. Dies muss ebenfalls in der Datei *CAPolicy.inf* geschehen.

Detaillierte Erläuterungen zum Inhalt der Datei *CAPolicy.inf* sind in der im Internet verfügbaren Herstellerdokumentation *Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure* zu finden.

Mitgliedschaft in der Gruppe *Zertifikatherausgeber*

Nur Zertifizierungs-stellencomputer dürfen Mitglied der Gruppe *Zertifikatherausgeber* sein

Die Mitgliedschaft in dieser Gruppe ermöglicht Computerkonten, Zertifikate in Benutzerobjekten zu veröffentlichen, d. h. diese Computer sind berechtigt, Zertifikate im Active Directory zu veröffentlichen. Dies trifft nur auf Zertifizierungsstellencomputer mit einer Active-Directory-integrierten

Zertifizierungsstelle zu, und nur diese sollten Mitglied dieser Gruppe sein. Die Mitgliedschaft in dieser Gruppe ist daher stetig zu überwachen.

Zugriffsberechtigungen auf Zertifikatsvorlagen

Sicherheit erhöhen mit Snap-In Zertifikatsvorlagen

Die Sicherheit kann bei entsprechendem Absicherungsbedarf (siehe Abschnitt "Absicherungsbedarf von Zertifizierungsstellen") erhöht werden, indem die Zugriffsberechtigungen auf Zertifikatsvorlagen auf bestimmte Benutzerkonten oder -gruppen eingeschränkt werden. Hierzu dient das Snap-In *Zertifikatsvorlagen*, welches manuell in die Microsoft Management Konsole (MMC) geladen werden muss. Die Berechtigungen auf Zertifikatsvorlagen können so eingeschränkt werden, dass Operationen wie das Anfordern oder das Ausstellen der Zertifikate nicht mehr von anderen Konten durchgeführt werden können.

Für Active-Directory-integrierte Zertifizierungsstellen können die Berechtigungen auf Zertifikatsvorlagen organisationsweit eingestellt werden:

Start | *Systemsteuerung* | *Verwaltung* | *Active Directory -Standorte und –Dienste* | Knoten *Services* | *Public Key Services* | *Certificate Templates*

Nach einer Standardinstallation dürfen Mitglieder der Gruppe *Authentifizierte Benutzer* die meisten Zertifikatstypen anfordern. Wenn die Zugriffsberechtigungen geändert werden sollen, dann sollte dies auf Grundlage eines Berechtigungskonzeptes erfolgen (siehe M 2.232 *Planung der Windows 2000/2003 CA-Struktur*).

Rollentrennung

Rollentrennung durchsetzen

Rollentrennung bedeutet, dass die Konzentration verschiedener bzw. aller kritischer Verwaltungsrollen im Zusammenhang mit einer PKI auf eine Person bzw. ein Benutzerkonto verhindert wird. Dies setzt eine Planung der Rollentrennung auf organisatorischer Ebene voraus. Für die technische Umsetzung kann die Rollentrennung automatisch vom System erzwungen (ab Windows Server 2003 Enterprise Edition) oder manuell realisiert werden. Das automatische Erzwingen hat jedoch weitreichende Auswirkung auf alle Komponenten der Zertifikatsdienste und ist nicht für alle Umgebungen geeignet. Weitere Hinweise zur Planung und Vorbereitung sind in M 2.232 *Planung der Windows 2000/2003 CA-Struktur* zu finden.

Zum Aktivieren/Deaktivieren der erzwungenen Rollentrennung dienen folgende Befehle an der Eingabeaufforderung:

```
certutil –setreg CA\SeparationEnabled 1
certutil –setreg CA\SeparationEnabled 0
```

Wird keine erzwungene Rollentrennung verwendet, sollten zumindest folgende Einstellungen manuell vorgenommen werden:

- alle Benutzer aus der Gruppe *Administratoren* entfernen, einschließlich des *Domänen-Admins*
- nur den oder die berechtigten Zertifizierungsstellen-Verwalter hinzufügen (sollten Mitglieder der Active Directory-Gruppe *Domänen-Admins* sein)
- *Start* | *Systemsteuerung* | *Verwaltung* | *Zertifizierungsstelle* | Eigenschaften der Zertifizierungsstelle | Reiter *Sicherheit* | für

Domänen-Admins und *Organisations-Admins* nur die Berechtigung *Zertifikate anfordern* aktivieren
- auf eine geeignete Rollentrennung auf organisatorischer Ebene achten

Es ist für jede Art der Rollentrennung das Erstellen von Sicherheitsgruppen zu empfehlen, welche die gewünschten Rollen repräsentieren. Die Administration wird dadurch erheblich erleichtert.

Schlüsselarchivierung

Die größte Gefahr unzureichender Rollentrennung entsteht, wenn gleichzeitig die Zertifizierungsstelle so konfiguriert wird, dass private Schlüssel nach dem Ausstellen von Zertifikaten auf der Zertifizierungsstelle archiviert werden (siehe M 2.232 *Planung der Windows 2000/2003 CA-Struktur)*. Wenn die Archivierung verwendet wird, ist die erzwungene Rollentrennung zu empfehlen. Wenn dies unter bestimmten Umständen nicht möglich ist, muss ein geeignetes Berechtigungskonzept implementiert werden. Insbesondere sollten die Exportberechtigung für private Schlüssel und die Berechtigung zur Schlüsselwiederherstellung nicht auf eine Person bzw. ein Benutzerkonto vereint sein, sonst kann eine einzelne Person private Schlüssel unerlaubt verwenden.

Ordnerberechtigungen

Ordnerberechtigungen einschränken

- **Ordner CertSrv:**

  Die Berechtigungen für den Ordner *%SystemRoot%\system32\certsrv* sollten so eingeschränkt werden, dass *SYSTEM* und *Administratoren* über das Recht *Vollzugriff* und *Authentifizierte Benutzer* über die Rechte *Lesen*, *Ausführen*, *Ordnerinhalt auflisten* und *Ordnerinhalt lesen* verfügen.

- **Ordner CertLog:**

  Die Berechtigungen für den Ordner *%SystemRoot%\system32\CertLog* sollten so eingeschränkt werden, dass *SYSTEM*, *Administratoren* und *Organisations-Admins* über das Recht *Vollzugriff* verfügen und keine weiteren Benutzer Berechtigungen erhalten.

- **Freigabe CertEnroll:**

  Die Berechtigungen für die Freigabe *CertEnroll* sollten so eingeschränkt werden, dass *SYSTEM*, *Administratoren* und *Organisations-Admins* über das Recht *Vollzugriff* verfügen und keine weiteren Benutzer Berechtigungen erhalten.

Veröffentlichungsintervalle für Sperrlisten

Verkürzen von Veröffentlichungs-intervallen

Die Sicherheit vor kompromittierten Sicherheitszertifikaten kann durch die Verkürzung der Veröffentlichungsintervalle von Sperrlisten und Deltasperrlisten erhöht werden.

Start | *Systemsteuerung* | *Verwaltung* | *Zertifizierungsstelle* | Name der Zertifizierungsstelle | *Gesperrte Zertifikate* | *Eigenschaften* | *Parameter für Sperrlistenveröffentlichung*

Hinweis: Deltasperrlisten enthalten nur die Änderungen seit der letzten Sperrlistenveröffentlichung. Aufgrund ihrer geringeren Größe können sie schneller und in kürzeren Intervallen abgerufen werden als

die vollständige Sperrliste. Deltasperrlisten sollten deshalb aktiviert bleiben.

Bei der Wahl eines geeigneten Intervalls spielen die im Abschnitt "Absicherungsbedarf für Zertifizierungsstellen" genannten Faktoren eine Rolle. Es ist hierbei zu bedenken, dass die Sperrlisten nach Ablauf des Veröffentlichungsintervalls nicht mehr gültig sind. Je nach Anwendung oder Komponente ist kein weiterer Betrieb möglich, bis eine aktuelle Sperrliste verfügbar ist, z. B. bei 802.1x-Authentisierung für *Wireless LAN* (WLAN). Je kürzer also die Veröffentlichungsintervalle, desto mehr Aufwand muss für die Verfügbarkeit von CDPs betrieben werden. Die Verlängerung des Intervalls über die Standardwerte (Sperrlisten eine Woche, Deltasperrlisten einen Tag) hinaus ist im Normalfall nicht zu empfehlen.

Handlungsanweisung bei Sicherheitsvorfall

Für den Fall der Kompromittierung eines Systembereiches, in dem Sicherheitszertifikate zum Einsatz kommen, sollte ein geeignetes Vorgehen definiert werden, um Missbrauch von Zertifikaten zu verhindern. Die Erstellung einer entsprechenden Handlungsanweisung ist zu empfehlen. Folgende Fragen sind besonders zu berücksichtigen:

- Wann ist der nächste effektive Sperrlisten-Veröffentlichungszeitpunkt?
- Welche Vorkehrungen gegen Missbrauch innerhalb des Veröffentlichungsintervalls sollen getroffen werden (z. B. Anhalten des Dienstes, der Applikation oder des administrativen Werkzeuges, das kompromittiert wurde)?
- Welche Dienste sind gegebenenfalls nicht mehr verfügbar, welche Dienste sind unter Umständen von der Deaktivierung einer Zertifizierungsstelle oder eines CDPs betroffen?

Aktivierung der Sperrlistenüberprüfung in Anwendungen

Es ist zu testen und darauf zu achten, dass Anwendungen innerhalb des betrachteten IT-Verbundes die Zertifikatssperrlisten der Windows-Server-2003-Zertifizierungsstellen überprüfen können.

Überwachung aktivieren

Start | *Systemsteuerung* | *Verwaltung* | *Zertifizierungsstelle* | Eigenschaften der Zertifizierungsstelle | Reiter *Überwachung* | alle Optionen aktivieren

Die Ereignisse werden im Ereignisprotokoll des Systems gespeichert und sind bei der regelmäßigen Auswertung zu überprüfen.

Dokumentation

Eine Mindestdokumentation sollte folgende Punkte enthalten:

- Welche Konten haben welche Verwaltungsrechte für die Zertifikatsdienste und für das CA-System?
- Welche Zertifizierungsstellen und welche Veröffentlichungspunkte gibt es und in welchem Bereich des betrachteten IT-Verbundes befinden sie sich?
- Von welchen administrativen Werkzeugen werden Zertifikate verwendet?
- Veröffentlichungsintervall der Sperrlisten
- Begründung für sonstige Abweichungen vom Installationsstandard

10 Auswahl geeigneter Lizenzierungsmethoden für Windows XP/Server 2003

Der Hersteller bietet verschiedene Lizenzprogramme an und versucht mit der so genannten Produktaktivierung und Lizenzschlüsseln den Einsatz lizenzierter Installationen zu kontrollieren. In diesem Zusammenhang ist die Gefährdung des IT-Grundschutzes G 2.28 *Verstöße gegen das Urheberrecht* zu nennen. Diese Faktoren beeinflussen den IT-Betrieb und somit die Beschaffungsentscheidung und sollten beim Auswahl- und Testverfahren für Windows Server 2003 berücksichtigt werden (siehe IT-Grundschutz Baustein B 1.10 *Standardsoftware*).

Grundbegriffe: Produktschlüssel und Produktaktivierung

Produktschlüssel

Lizenzschlüssel werden auch als Produktschlüssel bezeichnet und müssen während der Betriebssysteminstallation eingegeben werden. Ohne Produktschlüssel ist keine Installation möglich.

Produktaktivierung

Produktaktivierung ist eine Software-Prozedur zur Überprüfung des Produktschlüssels und zur endgültigen Freischaltung der installierten Software. Die Prozedur berechnet eine Installations-ID als Hash-Wert aus bestimmten Hardwarekennungen und dem Produktschlüssel, übermittelt diesen an Microsoft und erwartet eine Bestätigungs-ID zurück, um damit die Software endgültig freizuschalten. Die Hardwarekennungen werden durch die Hash-Wert-Bildung anonymisiert (siehe M 3.23 *Einführung in kryptographische Grundbegriffe*). Die Installations-ID und die Bestätigungs-ID können via Internet oder telefonisch durch den Server-Operator an den Hersteller übermittelt werden, wobei die Aktivierung via Internet mit einer vorbereiteten Installations-Routine automatisiert werden kann. Der Hersteller kann mittels Produktaktivierung die Anzahl der Installationen je Produktschlüssel einschränken und gegebenenfalls die Installation auf einem weiteren Computer verweigern.

Aktivierungsfrist

Nach Ablauf der Aktivierungsfrist ist der Server erst nach der Aktivierung wieder nutzbar. Die Aktivierungsfrist dauert normalerweise 30 Tage, bei einigen Lizenzvarianten länger.

Wirtschaftliche und administrative Gesichtspunkte

Durch die Produktaktivierung entsteht zusätzlicher organisatorischer und administrativer Aufwand, der bei der Beschaffung zu berücksichtigen ist. In IT-Umgebungen mit hohem Schutzbedarf sollte überprüft werden, ob die Produktaktivierung über Internet eine Gefährdung im Sinne des IT-Grundschutzes darstellt.

Im Folgenden werden die wirtschaftlichen und administrativen Gesichtspunkte verschiedener Beschaffungsmöglichkeiten für Lizenzen beleuchtet.

- **OEM-Lizenz**

  OEM-Lizenz

  Hersteller von Computersystemen liefern bei Verwendung einer OEM-Lizenz (Original Equipment Manufacturer) ein an ihre Hardware gebundenes Betriebsystem aus, welches meist betriebsfertig auf dem

Server vorinstalliert ist. Vorteile stellen die meist günstigen Konditionen für das Gesamtpaket und die ausgeschaltete Produktaktivierung dar. Nachteile sind:

- unflexible, an die jeweilige Serverhardware gebundene Lizenz
- Vorinstallation ist schlecht dokumentiert und genügt meist nicht dem IT-Grundschutz
- Installationsmedien fehlen oder enthalten angepasste Installations-Routinen, die meist ungeeignet und unzureichend dokumentiert sind, genügen meist nicht dem IT-Grundschutz
- spezielle, eingeschränkte Produktschlüssel
- starke Einschränkungen bei Sicherungs- und Wiederherstellungsszenarien
- schlecht geeignet für Verwaltung durch Softwaremanagement-Systeme

- **Lizenzprogramme**

Lizenzprogramme

Lizenzprogramme bieten verschiedene Möglichkeiten, um wirtschaftlichen und administrativen Anforderungen in höherem Maße gerecht zu werden, beispielsweise:

- bessere Konditionen für eine größere Anzahl von Lizenzen
- bessere Konditionen für zukünftige Produktaktualisierungen (Software Assurance)
- beschränkte Laufzeit für Lizenzen
- flexible Finanzierungsmodelle
- Installieren von Software zeitlich und organisatorisch unabhängig von der Lizenzbeschaffung
- kaufmännische Bestell- und Verwaltungswerkzeuge für Lizenzen

Lizenzprogramme berechtigen den Vertragspartner zur Nutzung so genannter Activation Centers von Microsoft, um von dort gültigem Produktschlüssel zu erhalten.

- **Einzel- und Mehrfachlizenzen mit Produktaktivierung**

Einzel- oder Mehrfach-Lizenz

Für eine Einzel- oder Mehrfach-Lizenz erhält man einen Produktschlüssel, der eine beschränkte Anzahl von Installation mit Produktaktivierung zulässt (siehe oben). Danach ist der Produktschlüssel an die Hardware gebunden. Dies stellt die gängige Lizenzierungsmethode für Windows Server 2003 in kleinen Umgebungen dar und kann mit einem Lizenzprogramm kombiniert werden. Wegen der Bindung des Produktschlüssels durch die notwendige Produktaktivierung ist bei Softwaremanagementsystemen und bei Sicherungs- und Wiederherstellungsszenarien ein erhöhter Aufwand einzuplanen. Die Bereitstellung von angepassten Installationsquellen über das lokale Netz ist nur eingeschränkt möglich.

- **Volumenlizenzprogramme**

  Volumenlizenz-programme

  Die höchste Flexibilität bieten Volumenlizenzprogramme sowohl hinsichtlich des Systemmanagements als auch bei der Beschaffung von Lizenzkontingenten. Microsoft stellt gesonderte Datenträger und so genannte Volumenlizenzschlüssel (VLK) für Vertragskunden zur Verfügung, mit denen eine große Zahl von Windows-XP/Server-2003-Systemen ohne Produktaktivierung installiert werden kann. Damit besteht bei diesem Modell keine Bindung zwischen Produktschlüssel und der individuellen Hardware.

  Der VLK muss vertraulich behandelt werden, da dessen Weitergabe an unberechtigte Dritte zu Missbrauch führen kann und gegen den Lizenzvertrag verstößt. Das gleiche gilt für Volumenlizenz-Datenträger.

- **Clientzugriffslizenzen**

  Clientzugriffslizenzen

  Clientzugriffslizenzen (CAL) berechtigen Clients und authentisierte Benutzer dazu, eine Verbindung zu einem Server (z. B. mit Windows Server 2003) herzustellen. Alle Windows-Server-2003-Editionen (mit Ausnahme der Web-Edition) benötigen CALs. Zwei grundlegende Arten werden unterschieden:

  0. Benutzer-CAL (neu bei Windows Server 2003), zu empfehlen, wenn einzelne Benutzer mehrere, verschiedene Client-Systeme nutzen
  0. Geräte-CAL, zu empfehlen, wenn sich mehrere Benutzer einzelne Client-Systeme teilen.

  Bei der wirtschaftlichen Betrachtung ist zu beachten, dass sich beide CAL-Varianten im Preis nicht unterscheiden. Ein Benutzer oder ein Gerät benötigt in einer Windows-2003-Server-Umgebung nur eine CAL. In der Praxis finden sich häufig Mischumgebungen oder längerfristige Migrationsszenarien, bei denen Windows Server 2003 parallel mit Windows 2000 Server oder NT 4.0 Server im Einsatz ist. Die unterschiedlichen Lizenzmodelle dieser Versionen und die vielfältigen Lizenzaktualisierungsmöglichkeiten erschweren es zum Teil erheblich, eine optimale oder mindestens ausreichende Lizenzierung für die Gesamtumgebung zu beschaffen. Für kleine bis mittlere Umgebungen sind Benutzer-CALs entsprechend der Anzahl der Mitarbeiter oft die einfachste und sicherste Variante. Bei einer Vermischung von Benutzer-CALs und Geräte-CALs sollten die Einsatzbereiche klar abgegrenzt und die Beschaffung unter finanziellen, organisatorischen und strategischen Gesichtspunkten sorgfältig geplant sein.

Dokumentation

Dokumentation

Die Beschaffung von Lizenzen ist so zu dokumentieren, dass Anzahl und Art der Lizenzen sowie zugehörige Lizenzprogramme jederzeit ersichtlich sind.

11 DHCP/DNS/WINS als Infrastrukturdienste unter Windows Server 2003

Die Protokolle *Dynamic Host Configuration Protocol* (DHCP), *Dynamic Name System* (DNS) und Windows *Internet Naming Service* (WINS) dienen unter Windows Server 2003 als zentrale Infrastrukturdienste für Namensauflösung und dynamische IP-Adressvergabe. Es sollte daher ein für diesen Einsatzzweck angepasstes Konzept erstellt werden. Vorrausetzungen für den sicheren und effektiven Einsatz der Infrastrukturdienste sind:

- Schulung der Administratoren in den Windows-Implementationen von DNS, DHCP, WINS und Active Directory
- vorhandenes IP-Konzept (Subnetze, Standorte), nähere Informationen siehe B 4.1 *Heterogene Netze*
- Entscheidung, ob und in welchen Bereichen dynamische IP-Adressvergabe in Frage kommt
- Prüfung, ob der Einsatz von Active Directory möglich ist
- Festlegung von Namensräumen bzw. Namensdomänen

In einer homogenen Windows-2000/XP/2003-Umgebung genügt bis zu einer gewissen Netzgröße ein gemeinsames Konzept für alle drei hier behandelten Dienste. Werden für einen der Dienste Produkte von Drittherstellern gewählt, sind jeweils eigene Konzepte für dynamische IP-Adressvergabe und Namensauflösung zu empfehlen. Das gleiche gilt, wenn Nicht-Windows-Plattformen bedient werden müssen oder wenn die Auflösung zusätzlicher, externer Namensräume mit einbezogen werden soll.

Analyse der Infrastruktur

Es ist nicht immer sinnvoll, alle mitgelieferten Sicherheitsfunktionen restriktiv einzustellen. Je mehr Plattformen bedient werden müssen, je mehr Abwärtskompatibilität zu älteren Windows-Versionen erforderlich ist und je mehr Flexibilität benötigt wird, desto weniger restriktiv können die Sicherheitsfunktionen von Windows Server 2003 genutzt werden. Als Vorbereitung sollten die unterschiedlichen System-Plattformen und die benötigte Flexibilität von Rechnern (Einsatzort, Häufigkeit von Ortswechseln oder Austausch, Art der Netzanbindung) analysiert werden. Die Konzepte stellen schließlich einen Kompromiss zwischen Betriebsfähigkeit und Sicherheit dar. Im Folgenden werden einige Sicherheitsaspekte erläutert, die berücksichtigt werden sollten.

> Hinweis: Das Erproben von Infrastrukturen in Testumgebungen ist selbst mit hohem Aufwand nur bedingt möglich. Konzeption und gegebenenfalls Testumgebung sollten daher nur von geschultem Fachpersonal durchgeführt werden.

Infrastrukturen in geschützten Netzbereichen betreiben

Infrastruktur durch Sicherheitsgateways schützen

Der Schutz vor Angriffen und Kompromittierung gegen Infrastrukturdienste und -informationen muss primär durch den Schutz des Netzbereiches mittels Sicherheitsgateways (siehe B 3.301 *Sicherheitsgateway (Firewall)*) und physische Netzzugangskontrolle gewährleistet sein. Infrastrukturdienste in exponierten Netzbereichen müssen von denen des geschützten Netzbereichs isoliert werden. Sollen Infrastrukturdienste in bestimmten Fällen dennoch grenzüberschreitend eingesetzt werden, ist für den Einzelfall (z. B. Internet-

DNS-Auflösung, DNS-Zonenübertragung in die DMZ, Split-DNS, DHCP für RAS-Verbindungen) ein geeignetes Sicherheitskonzept zu erarbeiten.

DHCP

DHCP dient unter Windows nicht nur der dynamischen Verwaltung von IP-Adressen, sondern wird auch für *Dynamisches DNS* (DDNS) benötigt. Ein DHCP-Client kommuniziert ohne Authentisierung und unverschlüsselt mit dem DHCP-Server.

Feste IP-Adressen für Infrastrukturserver, Autorisierung im Active Directory

Auf Servern mit hohem Schutzbedarf sollten DHCP-Client und Server-Dienst deaktiviert werden. Server mit Infrastrukturdiensten müssen feste IP-Adressen haben. Der DHCP-Server-Dienst sollte nicht auf einem Domänencontroller installiert werden. Wird Active Directory verwendet, sollten alle Windows-DHCP-Server autorisiert werden (Konsole *DHCP*: *Start* | *Systemsteuerung* | *Verwaltung* | *DHCP* | Menüpunkt *Aktion* | *Autorisierte Server verwalten…* | IP-Adressen der Server hinzufügen).

Unerwünschte DHCP-Server im Netz

Andere DHCP-Server sollten strikt von DHCP-Servern unter Windows 2000 Server bzw. Windows Server 2003 isoliert werden (durch Netzsegmentierung, logische Segmentierung). Es muss sichergestellt werden, dass im betrachteten Netz-Bereich keine unberechtigten DHCP-Server-Dienste (so genannte *Rogue*-Server) aktiv sind. In solchen Fällen enthalten die System-Ereignisanzeigen von DHCP-Clients und DHCP-Servern sowie die DHCP-Protokolldateien auf dem Server eine erhöhte Anzahl DHCP-Fehler. In den Protokolldateien (Verzeichnis *C:\WINDOWS\system32\dhcp*) werden Ereignisnummern über 50 für *Rogue*-Servererkennungsinformationen verwendet. Dies ist bei der regelmäßigen Durchsicht der Protokolle zu berücksichtigen.

Sicherheitsaspekte der Leasedauer

Für die *Leasedauer* (Gültigkeitszeitraum für eine dynamisch zugewiesene IP-Adresse) muss ein geeigneter Kompromiss zwischen

- Anzahl der Clients und dem zur Verfügung stehenden Adressbereich (z. B. könnte der Einsatz vieler Remote-Access-Clients (RAS) ein Grund für eine kürzere Leasedauer sein)
- Häufigkeit des Ortswechsels oder des Austauschs von Clients
- Sicherheitsaspekten

gefunden werden. Dafür ist einschlägige Fachliteratur zu DHCP sowie das Internetstandard-Dokument RFC 2131 heranzuziehen. Zu den Sicherheitsaspekten gehört unter anderem die Protokollierung des Netzverkehrs. Die Auswertung der Protokolle von Netzwerkmonitoren anhand von IP-Adressen wird durch häufig wechselnde IP-Adressen stark erschwert. Bei erhöhtem Schutzbedarf ist zu überlegen, die standardmäßige Leasedauer von 8 Tagen auf wesentlich höhere Werte (z. B. 180 Tage) oder auf *unbegrenzt* zu setzen (Konsole *DHCP* | jeweiliger Server | *Eigenschaften* des Bereiches | *Leasedauer für DHCP-Clients*). Lange Leasedauern können allerdings bei DDNS zum Sicherheitsrisiko werden (siehe auch Abschnitt "DDNS").

Herstellerspezifische Optionen

In den herstellerspezifischen Bereichsoptionen für DHCP ist es sinnvoll, das Feld 046 (*WINS/NBT-Knotentyp*) auf den Wert 8 (*H-Node*) zu setzen. In den Feldern 06 (DNS) bzw. 044 (WINS) sollten erreichbare Namensserver übergeben werden. Ziel ist es, durch Namensauflösung verursachte IP-

Broadcasts zu vermeiden. Mit dem Wert 2 im Feld 001 (*NetBT*) kann die NetBIOS-Namensauflösung komplett deaktiviert werden. Bei der Planung der weiteren herstellerspezifischen Optionen ist abzuwägen, welche der Einstellungen alternativ oder zusätzlich über Gruppenrichtlinien des Active Directory bereitgestellt werden können (siehe auch Abschnitt "Verwaltung und Konfiguration").

Feste IP-Adressen in der DHCP-Konsole erfassen

Feste IP-Adressen sollten als Ausschlussbereiche oder Reservierungen in die DHCP-Konsole eingetragen werden. Dies erhöht die Übersichtlichkeit und verhindert DHCP-Konflikte durch Fehlkonfiguration der Bereiche.

DNS

Planung der DNS-Namensstruktur

Zunächst muss die Planung der DNS-Namensstruktur abgeschlossen werden. Dazu sind nicht nur die klassischen DNS-Parameter wie Namensräume, Zonen, Reverse-Lookup, Delegierungen, Weiterleitungen, Rekursion und Stammhinweise zu planen, sondern auch die DNS-Servertypen und die Art der Auflösung festzulegen. Zu nennen sind hierbei Stub-Zonen, bedingte Weiterleitung und DNS-Cache-Server. Die Gesichtspunkte Verfügbarkeit der DNS-Informationen (siehe Abschnitt "Verfügbarkeit"), Performance bei der Auflösung von Clientanfragen und Verwaltungsaufwand sollten berücksichtigt werden.

Active-Directory-integrierte Zonen

Die höchste Sicherheit bei angemessenem Aufwand wird erreicht, wenn ausschließlich Active-Directory-integrierte Zonen verwendet und korrekt konfiguriert werden. Der DNS-Server muss dann aber Domänencontroller sein. Dateibasierte DNS-Datenbanken sollten vermieden werden. Dann können wichtige Sicherheitsfunktionen flächendeckend aktiviert werden. Die wichtigsten sind:

- *Secure Dynamic Update* (Authentisierung für dynamische Aktualisierung von DNS-Einträgen erforderlich)
- Zugriffskontrolle auf Einträge
- Zugriffsüberwachung auf Einträge (SACL)
- Multi-Master-Replikation (geringerer Verwaltungsaufwand als bei einer separaten Master/Slave-Topologie für DNS-Daten)
- Globale DNS-Partitionen im Active-Directory-Forrest (Schaffung hoher Redundanz zur Erhöhung der Verfügbarkeit)
- Active-Directory-Mechanismen für Speicherung und Replikationsverkehr schützen die Vertraulichkeit der DNS-Daten wesentlich besser als dateibasierte DNS-Datenbanken

Zonenübertragung möglichst deaktivieren

Die Zonenübertragung (Master/Slave-Replikation) sollte deaktiviert bleiben (Konsole *DNS*: *Start* | *Systemsteuerung* | *Verwaltung* | *DNS* | *Eigenschaften* einer DNS-Zone auswählen | *Zonenübertragung*). Master/Slave-Replikation sollte nur verwendet werden, wenn DNS-Daten

- mit anderen Plattformen (z. B. UNIX)
- auf Windows-Server, die nicht Domänencontroller sind (z. B. bei erhöhtem Schutzbedarf von exponierten Servern)

repliziert werden müssen. Die Liste der für die Zonenübertragung autorisierten Server sollte jedoch so kurz wie möglich gehalten werden. Ein gleichwertiger Schutz von DNS-Daten wie bei Active-Directory-integrierten Zonen ist nicht möglich. Restriktivere Zugriffsberechtigungen auf die DNS-Datenbankdateien und den Server allgemein, intensivere Überwachung der DNS-Ereignisse

(Entdeckung von Spoofing-Versuchen, unerlaubtem Zonentransfer, unerlaubten dynamischen Updates) sowie Verschlüsselung des Netzverkehrs können die Sicherheit jedoch verbessern. Neben einem geeigneten technischen Konzept für diesen Modus sollte in einer IT-Sicherheitsrichtlinie festgelegt sein, ob und unter welchen Bedingungen dateibasierte Master/Slave-Replikation eingesetzt werden darf.

> Hinweis: Sekundäre Zonen können nicht in das Active Directory integriert werden. In vielen Fällen erfüllen Stub-Zonen den gleichen Zweck und sollten dann bevorzugt werden.

DNS-Cache schützen

Die standardmäßige Option *Cache vor Beschädigungen sichern* sollte aktiviert bleiben (Konsole *DNS* | *Eigenschaften* des Servers | *Erweitert*).

Clients ohne DNS-Unterstützung

Befinden sich in einem Netz Clients ohne DNS-Unterstützung, sollte *WINS*- und *WINS-R-Lookup* aktiviert werden, falls Namensauflösung für diese Clients benötigt wird. Es ist nicht zu empfehlen, diese Eintragstypen bei Zonentransfers mit zu replizieren. Die Einstellungen sind in der Konsole *DNS* | *Eigenschaften* der Zone | Registerkarte *WINS* zu finden.

DDNS

DDNS ist ein potentielles Risiko

Dynamic Domain Name System (DDNS) erstellt automatisch DNS-Einträge für Clients. DDNS ist für Active Directory erforderlich und erleichtert außerdem die Verwaltung von DNS-Clients. In Hochsicherheitsumgebungen kann DDNS jedoch ein Risiko darstellen. Hier ist zu überlegen, DDNS nur während der Bereitstellung zu verwenden (bis alle erforderlichen Einträge im DNS registriert sind) und anschließend zu deaktivieren. Statische Einträge können jederzeit hinzugefügt werden.

> Konsole *DNS*: *Start* | *Systemsteuerung* | *Verwaltung* | *DNS* | *Eigenschaften* der Zone | *Allgemein* | *dynamische Updates* auf *keine* setzen

Option *Nur sichere* Einträge

Für den normalen Client/Server-Betrieb sind die Modi *Nicht sichere und sichere* und *Nur sichere* relevant. Nur letztere Option schützt effektiv gegen DNS-Spoofing und missbräuchliches Ändern oder Hinzufügen von DNS-Einträgen. Sie ist zu empfehlen, ist aber nur in Active-Directory-integrierten Zonen aktivierbar und funktioniert nur in reinen Windows 2000/XP/2003-Umgebungen. Für andere Clients kann die dynamische Aktualisierung und Authentisierung vom DHCP-Server als *DNS-Update-Proxy* durchgeführt werden (Registerkarte *DNS* in der Konsole *DHCP*: *Start* | *Systemsteuerung* | *Verwaltung* | *DHCP* | *Eigenschaften* des DHCP-Servers). Aufgrund fehlender Authentisierung zwischen Client und DHCP-Server ist die Schutzwirkung jedoch gering.

Alternativen für sichere Einträge in heterogenen Netzen

Ein sicherer DNS-Eintrag kann ausschließlich vom Besitzer des Eintrages geändert werden. Der Aufwand zum Durchsetzen nur sichererer Einträge in heterogenen Umgebungen kann erheblich sein. Es ist daher zu überlegen, ob der Schutz der Infrastruktur durch Vorkehrungen auf anderer Ebene (siehe Abschnitt "Infrastrukturen in geschützten Netzbereichen betreiben") ausreichend gewährleistet ist und nicht sichere Einträge toleriert werden können.

Für sichere Einträge ist konzeptionell zu berücksichtigen:

- Alterungsintervalle und Aufräumvorgänge festlegen (standardmäßig deaktiviert)
- Zusammenspiel mehrerer DHCP-Server und mobiler Clients planen, Ausfall eines DHCP-Servers berücksichtigen
- Verwendung der Sicherheitsgruppe *DnsUpdateProxy* für DHCP-Server und andere Rechner in Erwägung ziehen
- gegebenenfalls verstärkte Zugriffsrechte (ACL) und Überwachungseinstellungen (SACL) für Einträge von besonders schützenswerten Rechnern

Bei Einsatz des DHCP-Servers als *DNS-Update-Proxy* sollte die Option *A- und PTR-Einträge beim Löschen der Lease verwerfen* aktiviert sein (Registerkarte *DNS* in der Konsole *DHCP* | *Eigenschaften* des DHCP-Servers). Für dynamisch aktualisierte Einträge sollte eine kurze Alterung eingestellt sein (Konsole *DNS* | *Eigenschaften* der Zone | *Allgemein* | *Alterung…*). Der Standardwert von einer Woche bietet ausreichende Sicherheit für die meisten Szenarien.

WINS

Nur aus Kompatibilitätsgründen einsetzen

WINS dient der Vermeidung von IP-Broadcasts von NetBIOS-Diensten. Diese werden von Windows NT3.5/4.0 und Windows 9x sowie Geräten und Software von Drittherstellern verwendet. Die Verwendung von NetBIOS als Infrastrukturdienst ist veraltet und anfällig für Angriffe und Fehlfunktionen. Die NetBIOS-Namensauflösung kann unter Windows Server 2003 und Windows XP vollständig durch DNS ersetzt werden. WINS sollte daher auf Systeme beschränkt werden, wo dies aus Kompatibilitätsgründen benötigt wird. In Netzbereichen mit hohen Sicherheitsanforderungen sollten NetBIOS-Namensauflösung bzw. WINS auf allen Clients und Servern deaktiviert werden.

Sicherheitsrisiken

Eine gleichwertige Sicherheit des WINS-Namensdienstes wie bei DNS mit Active-Directory-integrierten Zonen ist nicht möglich. Einige Sicherheitsrisiken sind:

- dynamische Aktualisierung von Einträgen ohne Authentisierung
- ungeschützte Replikation
- kein Abbilden von Standortstrukturen möglich
- WINS-Replikation ist anfällig für Inkonsistenzen
- unnötige parallele Struktur zu DNS, was zu Inkonsistenzen und Sicherheitslücken führt

Vorkehrungen

Zur Erhöhung der Sicherheit sollten daher die gleichen Vorkehrungen wie bei Datei-basiertem DNS mit Master/Slave-Replikation ergriffen werden (siehe Abschnitt "DNS"). Folgende WINS-spezifische Punkte sind zusätzlich zu berücksichtigen:

1) Replikation ist nur mit definierten Partnern erlaubt (Konsole *WINS*: *Start* | *Systemsteuerung* | *Verwaltung* | *WINS* | Server auswählen | *Eigenschaften* vom Knoten *Replikationspartner* | Option *Replikation nur mit Partnern* aktivieren)

2) Alterungsintervalle und Aufräumintervalle, in denen abgelaufene dynamische Einträge und gelöschte Einträge entfernt werden, so klein

wie möglich festlegen, an Standardwerten orientieren (Konsole *WINS* | *Eigenschaften* des Servers | *Intervalle* | *Wiederherstellen*)

0) Art der Außerbetriebnahme eines WINS-Servers festlegen, damit verwaiste Einträge auf anderen WINS-Servern vermieden werden, gegebenenfalls Handlungsanweisung erstellen (Details siehe Hilfethema *Außerbetriebnahme eines WINS-Servers* der integrierten Windows-Hilfe)

0) Anzahl der Einträge auf die benötigten Rechner beschränken (z. B. durch Netz-Segmentierung oder Deaktivierung nicht benötigter WINS-Clients via Gruppenrichtlinien)

0) statische Einsträge für besonders schützenswerte Rechner erstellen (Automatische Registrierung bei diesen WINS-Clients wenn möglich deaktivieren, da deren Einträge sonst fehlerhaft repliziert werden)

WINS sollte nicht unvorbereitet aus dem Netz entfernt werden. Die Konsole *WINS* | Kontextmenü des Servers | *Serverstatistik anzeigen* zeigt das aktuelle Aufkommen von Client-Abfragen an. Es muss analysiert werden, welche Rechner, Geräte, Dienste und Anwendungen Namensauflösung benötigen. Für diese muss das flächendeckende Funktionieren von DNS sichergestellt sein. Der Umgang mit Geräten, die nur NetBIOS-Namensauflösung unterstützen, sollte in einer Richtlinie definiert sein. Das Infrastrukturkonzept muss enthalten, wie NetBIOS-Namensauflösung und IP-Broadcasting in diesen Fällen beschränkt eingesetzt werden können.

Verfügbarkeit

Redundante Namensserver

Durch den Ausfall eines Infrastrukturdienstes kann der ganze Netzbetrieb zum erliegen kommen. Deshalb ist hohe Verfügbarkeit erforderlich. In einem Netzbereich sind mehrere DNS- und WINS-Server möglich, die sich miteinander replizieren (d. h. abgleichen). Für eine Namensdomäne sollten immer wenigstens zwei Repliken auf unterschiedlicher Hardware vorhanden sein. Auf allen Rechnern müssen mindestens zwei Namensserver eingetragen sein, die über das LAN oder eine adäquate Netzanbindung erreichbar sind.

Verfügbarkeit von DHCP erhöhen

DHCP-Server können nicht auf die gleiche Weise redundant gehalten werden, da nur ein aktiver DHCP-Server pro IP-Adressbereich möglich ist. Die Alternativen unterscheiden sich hinsichtlich Aufwand und Verfügbarkeit (siehe auch M 2.314 *Verwendung von hochverfügbaren Architekturen für Server*). Es kann z. B. ein Hochverfügbarkeitscluster unter Windows Server 2003 Enterprise Edition aufgebaut werden. Mit geringerem Aufwand sind Hot-Standby-Lösungen mit manuellem Umschwenken realisierbar: Innerhalb einer Domäne können mehrere DHCP-Server autorisiert (siehe Abschnitt "DHCP") und für den gleichen IP-Adressbereich konfiguriert werden, jedoch wird nur auf einem Server der IP-Adressbereich aktiviert. Bei Ausfall des aktiven Servers wird der Bereich manuell auf einem anderen Server aktiviert. Es können auch mehrere DHCP-Server gleichzeitig aktiv sein, solange sie für unterschiedliche Teile des insgesamt zur Verfügung stehenden IP-Adressbereichs konfiguriert sind. Dann muss allerdings der nach Ausfall eines DHCP-Servers verbleibende IP-Adressbereich immer noch genügend freie IP-Adressen enthalten. Letztere Variante bietet auch einen gewissen Schutz

gegen *Denial-of-Service*-Attacken (DoS) auf DHCP-Server. In jedem Fall ist eine geeignete Strategie zu wählen und umzusetzen.

Verwaltung und Konfiguration

Einsatz von Rollenteilung bei der Administration

Infrastrukturdienste beeinflussen stark die Verfügbarkeit und Integrität des IT-Verbundes. In größeren Umgebungen sollte überlegt werden, für die Administration eine Rollenteilung einzuführen (siehe M 2.364 *Planung der Administration für Windows Server 2003*), z. B. um Standort-Administratoren oder Support-Personal nicht mit vollen administrativen Rechten für den Server oder die Domäne ausstatten zu müssen und um eine effektivere Überwachung der Ausübung von Rechten zu erzielen. Die vordefinierten Sicherheitsgruppen *DHCP-Benutzer* und *WINS-Benutzer* ermöglichen Einsicht in die Konsolen und Protokolle, aber ohne Schreibzugriff. *DHCP-Admins* (lokale Gruppe) und *DNS-Admins* (lokale Domänengruppe) können die Infrastrukturdienste dediziert administrieren. Berechtigungen für die Administration der Infrastrukturdienste sollten so eingeschränkt wie möglich vergeben werden.

Gruppenrichtlinien statt DHCP-Bereichsoptionen

Mit Gruppenrichtlinien können die besprochenen Einstellungen für Infrastrukturclientdienste z. T. effizienter und zielgerichteter in größeren Umgebungen verteilt werden als mit DHCP-Bereichsoptionen. Sie bieten Authentisierung und nutzen gegebenenfalls vorhandene Netzverschlüsselung aus. Einige Einstellungen stehen in den mitgelieferten administrativen Vorlagen in der Rubrik *Netzwerk* | *DNS-Client* zur Verfügung. Dies sollte zur Erhöhung der Sicherheit überlegt werden.

Datensicherung, Aufbewahren von Protokolldateien

Sämtliche Protokolldateien und die Datenbanken der Dienste (z. B. DHCP-Datenbank) werden von der Systemstatussicherung berücksichtigt (siehe M 6.99 *Regelmäßige Sicherung wichtiger Systemkomponenten für Windows Server 2003*), sofern sie sich im Windows-Systemverzeichnis befinden. Sie sollten dort belassen werden, da restriktive Berechtigungen speziell für die Datenbankdateien voreingestellt sind, welche an einem anderen Speicherort erst nachgebildet werden müssten. Anhand der Protokolle von Infrastrukturdiensten lassen sich viele Vorgänge im Netz nachvollziehen, z. B. bei Sicherheitsvorfällen. Daher ist für Protokolle die Aufbewahrungsfrist in einer Sicherheitsrichtlinie zu definieren.