GCCSI

Ihr Dienstleister in:

Gürbüz Computer Consulting & Service International 1984-2007 l Önder Gürbüz l Aar Strasse 70 l 65232 Taunusstein
info@gccsi.com l +49 (6128) 757583 l +49 (6128) 757584 l +49 (171) 4213566

Bedrohungen und Gegenmaßnahmen: Sicherheitseinstellungen unter Windows Server 2003 und Windows XP

Microsoft® Solutions for Security

Danksagung

Die Microsoft Solutions for Security Gruppe (MSS) möchte dem Team dieses Handbuches seinen Dank und seine Anerkennung aussprechen. Die folgenden Personen waren für die Entwicklung, das Schreiben und das Testen dieses Handbuches direkt verantwortlich, oder haben dazu Beigetragen.

Autor

Kurt Dillard

Inhaltliche Mitarbeit

William Dixon

Eric Fitzgerald

Jesper Johansson

José Maldonado

Brad Warrender

Tester

Kenon Bliss

Korrektur

Rich Benack

Robert Hensing

Ben Smith

Jeff Williams

Mitarbeiter

Ignacio Avellaneda

Ganesh Balakrishnan

Derick Campbell

Flicka Crandell

Paresh Gujar

Vince Humphreys

Ashish Java

Herausgeber

Reid Bannecker

John Cobb

Jon Tobey

Programmanager

Chase Carpenter

Joanne Kennedy

Kelly McMahon

Jeff Newfeld

Rob Oikawa

Bill Reid

Sandeep Sinha

Bomani Siwatu

Graham Whiteley

Auf Anfrage von Microsoft beteiligten sich das *Center for Internet Security (CIS)* und das *United States Department of Commerce National Institute of Standards and Technology (NIST)* an der Überarbeitung dieses Handbuches und stellten Dokumente zur Verfügung, die in die Veröffentlichung mit eingeflossen sind. Microsoft möchte außerdem dem *Siemens Workplace Architecture Team* und *National Broadband LLC* für die wertvollen Beiträge und Informationen bei der Arbeit an diesem Handbuch danken.

Inhaltsverzeichnis

1

Einführung

Zweck dieses Handbuches ist es, Ihnen ein Nachschlagewerk zu den möglichen Sicherheitseinstellungen der aktuellen Microsoft® Windows® Betriebssysteme zur Verfügung zu stellen. Es handelt sich um ein Begleithandbuch zu zwei anderen Publikationen von Microsoft: Das *Windows Server 2003 Sicherheitshandbuch* unter http://www.microsoft.com/germany/ms/technetdatenbank/overview.asp?siteid=600215 und das *Windows XP Sicherheitshandbuch*. Viele der Gegenmaßnahmen dieses Handbuches werden in diesen beiden Handbüchern für bestimmte Serverrollen gar nicht umgesetzt. Dies geschieht, um deren Verwendbarkeit, Verwaltbarkeit, Verfügbarkeit, Leistung und Kompatibilität sicherzustellen. Auch wenn es schon oft gesagt wurde, soll doch noch einmal daran erinnert werden, dass es sich bei Sicherheit und Funktionalität um zwei gegensätzliche Extreme handelt. Wenn die Sicherheit verbessert wird, verschlechtert sich die Funktionalität und anders herum. Obwohl es Ausnahmen von dieser Regel gibt - einige Sicherheitsmaßnahmen verbessern sogar die Funktionalität - ist sie in den meisten Fällen zutreffend.

Die Kapitel dieses Handbuches sind so aufgeteilt, dass sie ungefähr den Hauptabschnitten des Gruppenrichtlinieneditors entsprechen. Jedes Kapitel beginnt mit einer kurzen Zusammenfassung des Inhalts, dann folgt eine Auflistung der jeweiligen Unterabschnitte. Jeder dieser Unterabschnitte entspricht einer der Einstellungen, die in der unten beschriebenen Excel-Tabelle aufgeführt sind. Die jeweiligen Maßnahmen werden jeweils kurz beschrieben. Innerhalb der einzelnen Unterabschnitte gibt es für jede Einstellung drei weitere Unterabschnitte: *Sicherheitslücken, Gegenmaßnahmen* und *Mögliche Auswirkungen.* Der Abschnitt *Sicherheitslücken* beschreibt, wie eine unsichere Konfiguration von einem Angreifer ausgenutzt werden kann. Der Abschnitt *Gegenmaßnahmen* beschreibt, wie diese implementiert werden können, und der Abschnitt *Mögliche Auswirkungen* zeigt schließlich die möglichen negativen Auswirkungen der Gegenmaßnahme.

Kapitel 2, *Richtlinien auf Domänenebene*, beginnt zum Beispiel mit den folgenden Abschnitten:

- Kontenrichtlinien
    - Kennwortchronik erzwingen
        - Sicherheitslücken
        - Gegenmaßnahmen
        - Mögliche Auswirkungen
    - Maximales Passwortalter
        - Sicherheitslücken
        - Gegenmaßnahmen
        - Mögliche Auswirkungen

Dieses Muster wiederholt sich im gesamten Handbuch. Einstellungen, die in engem Zusammenhang stehen, werden in einen einzelnen Abschnitt zusammengefasst. In Kapitel 5: *Sicherheitsoptionen* werden zum Beispiel die folgenden vier Einstellungen im Abschnitt *Microsoft Netzwerk Client und Server: Digitale Kommunikation signieren (vier Einstellungen)* zusammengefasst:

- Microsoft-Netzwerk (Client): Kommunikation digital signieren (immer)
- Microsoft-Netzwerk (Client): Kommunikation digital signieren (wenn Server zustimmt)
- Microsoft-Netzwerk (Server): Kommunikation digital signieren (immer)
- Microsoft-Netzwerk (Server): Kommunikation digital signieren (wenn Client zustimmt)

Es werden zwar viele der in einer Gruppenrichtlinie möglichen Einstellungen besprochen, jedoch nicht alle. Dies liegt daran, dass viele Einstellungen einer Gruppenrichtlinie für Verwaltungszwecke gedacht sind und sie im Bezug auf Sicherheit nicht relevant sind. Es werden ausschließlich die Einstellungen und Features von Microsoft Windows Server 2003 und Windows XP besprochen, die bei der Absicherung verwendet werden können.

Dieses Handbuch soll Sie und Ihre Organisation bei der Entscheidung unterstützen, welche Maßnahmen mit welcher Priorität umgesetzt werden sollen. Die Standardeinstellungen sind in der Excel-Tabelle *Windows Standardeinstellungen für Sicherheit und Dienste.xls* aufgeführt. Das erste Arbeitsblatt, *Windows Server 2003 Standard,* enthält die unter Windows Server 2003 verfügbaren Gruppenrichtlinieneinstellungen. Die Spalten haben die folgende Bedeutung:

- Spalte H (angezeigter Einstellungsname): Der Name der Einstellungen, der im Snap-In Windows Server 2003 Gruppenrichtlinieneditor angezeigt wird.
- Spalte J (Default Domain Policy): Der Wert in der bereits vorhandenen Default Domain Policy. Diese wird erstellt, wenn Sie den ersten Domänencontroller einer neuen Active Directory® Domäne einrichten.
- Spalte K (Default Domain Controller Policy): Der Wert in der bereits vorhandenen Default Domain Controller Policy. Diese wird erstellt, wenn Sie den ersten Domänencontroller einer neuen Active Directory® Domäne einrichten.
- Spalte L (Standardeinstellungen für eigenständige Server): Die Standardwerte für eigenständige Server unter Windows Server 2003.
- Spalte M (Effektive Standardeinstellungen für Domänencontroller): Der effektive Wert für Domänencontroller bei aktiven Standardeinstellungen.
- Spalte N (Effektive Standardeinstellungen für Mitgliedsserver): Der effektive Wert für Mitgliedsserver bei aktiven Standardeinstellungen.

Mit „Effektive Standardeinstellungen“ sind die Einstellungen gemeint, die ohne Änderungen der Sicherheitseinstellungen aktiv sind. Die effektive Einstellung wird durch die Gruppenrichtlinien-Engine durch die Abarbeitung der Gruppenrichtlinien beim Start des Computers festgelegt. Die Engine verarbeitet die Einstellungen in der im Abschnitt *Anwendung der Gruppenrichtlinien* von *Kapitel 2: Konfigurieren der Domäneninfrastruktur*, beschriebenen Priorität. Um die Lesbarkeit der Tabelle zu fördern, wurde dort die im Gruppenrichtlinieneditor verwendete Hierarchie nachgebildet.

Die zweite Tabelle, *Windows 2003 Systemdienste,* listet alle unter Windows Server 2003 verfügbaren Dienste auf. Sie enthält die folgenden Spalten:

- Spalte A (vollständiger Dienstname): Der Name des Dienstes, wie er in der Microsoft Management Konsole (MMC) *Dienste* angezeigt wird.
- Spalte B (Dienstname): Enthält den Kurznamen des Dienstes. Dieser wird zum Beispiel in vielen Kommandozeilentools verwendet.
- Spalte C (Starttyp auf Domänencontrollern): Gibt den Standardstartyp auf einem Windows Server 2003 Domänencontroller an.
- Spalte D (Starttyp auf Mitgliedsservern): Gibt den Standardstartyp auf einem Windows Server 2003-Computer, der Mitglied einer Active Directory basierten Domäne ist, an.
- Spalte E (Starttyp auf eigenständigen Servern): Gibt den Standardstartyp auf einem eigenständigen Server unter Windows Server 2003 an.
- Spalte H (Konto): Gibt das Konto an, dass der Dienst bei der Standardkonfiguration verwendet.

Es gibt zwei zusätzliche Tabellen: *Windows XP Standard* und *Windows XP Systemdienste*. Diese sind genauso formatiert, und sie enthalten die Sicherheitseinstellungen und Dienste unter Windows XP.

2

Richtlinien auf Domänenebene

Alle Kontenrichtlinieneinstellungen der Gruppenrichtlinien werden auf Domänenebene angewandt. In der vorgegebenen *Default Domain Controller Policy* gibt es für die Kontenrichtlinien, Kontosperrungsrichtlinien und Kerberos-Richtlinien bereits Standardeinstellungen. Bedenken Sie bei der Konfiguration dieser Richtlinien, dass Microsoft Windows nur eine Domänen-Kontenrichtlinie erlaubt. Und zwar die Kontenrichtlinie, die der Stammdomäne der Struktur zugewiesen ist. Sie wird zur Standard-Kontenrichtlinie aller Windows-Systeme, die Mitglied der Domäne sind. Die einzige Ausnahme dieser Regel ist die Definition einer weiteren Kontenrichtlinie für eine Organisationseinheit. Sie wirkt sich auf die lokalen Richtlinien aller Computer der Organisationseinheit aus. Die entsprechenden Einstellungen werden in diesem Kapitel besprochen.

Kontenrichtlinien

Kontenrichtlinien werden auf Domänenebene implementiert. Eine Microsoft Windows Server 2003-Domäne benötigt jeweils eine einzelne Passwortrichtlinie, eine Kontosperrungsrichtlinie und eine Kerberosrichtlinie für die gesamte Domäne. Wenn diese Richtlinien auf irgendeiner anderen Ebene konfiguriert werden, sind hiervon nur die lokalen Konten auf Mitgliedsservern betroffen. Wenn es Gruppen gibt, für die separate Passwortrichtlinien notwendig sind, sollten diese in eine zusätzliche Domäne oder eine andere Gesamtstruktur verschoben werden.

Unter Windows wird, genau wie bei vielen anderen Betriebssystemen, normalerweise die Authentifizierung eines Benutzers über ein Passwort oder eine Passphrase (zum Beispiel ein ganzer Satz statt eines einzelnen Passwortes) durchgeführt. Die Absicherung Ihrer Netzwerkumgebung setzt voraus, dass alle Benutzer starke Passwörter verwenden. So wird vermieden, dass nicht autorisierte Benutzer die Möglichkeit haben, schwache Passwörter zu erraten, oder ein Benutzerkonto mit Hilfe eines Tools zu kompromittieren.

Ein komplexes Passwort, das regelmäßig geändert wird, reduziert die Wahrscheinlichkeit eines erfolgreichen Passwortangriffs. Passwortrichtlinien regeln die Komplexität und Lebensdauer von Passwörtern. Die einzelnen Einstellungen der Passwortrichtlinien werden in diesem Abschnitt besprochen.

> **Anmerkung:** Für Domänenkonten kann es pro Domäne nur eine Kontenrichtlinie geben. Diese muss in der *Default Domain Policy*, oder in einer neuen Richtlinie, die der Domäne zugewiesen ist und eine höhere Priorität als die *Default Domain Policy* hat, definiert sein. Domänencontroller holen die Kontenrichtlinien immer aus der Gruppenrichtlinie, die auf die Domäne zugewiesen ist. Auch wenn es für die Domänencontroller-OU eine andere Gruppenrichtlinie gibt.

Die Arbeitsstationen und Server, die der Domäne beitreten, erhalten normalerweise für ihre lokalen Konten die gleiche Kontenrichtlinie. Wenn allerdings für die OU, in der sich die Computer befinden, Kontenrichtlinien definiert sind, dann können diese von der *Default Domain Policy* abweichen.

Die Einstellungen der Kontenrichtlinien können im Gruppenrichtlinieneditor über den folgenden Pfad konfiguriert werden:
Computerkonfiguration\Windows Einstellungen\Sicherheitseinstellungen\Kontenrichtlinien\Passwortrichtlinien

Kennwortchronik erzwingen

Diese Einstellung legt fest, wie viele Passwörter verwendet werden müssen, bevor ein altes Passwort wiederverwendet werden kann.

Die Möglichen Einstellungen sind:

- **Ein benutzerdefinierter Wert zwischen 0 und 24**
- **Nicht konfiguriert**

Sicherheitslücken

Die Wiederverwendung von Passwörtern ist in jeder Organisation ein wichtiges Thema. Viele Benutzer möchten ihre Passwörter am liebsten immer wieder verwenden. Wenn für ein Konto jedoch länger das gleiche Passwort genutzt wird, dann erhöht sich die Chance, dass ein Angreifer das Passwort über einen Brute-Force-Angriff herausfindet. Wenn die Benutzer zwar ihr Passwort ändern müssen, sie aber nicht an der Wiederverwendung des alten Passworts gehindert werden, oder wenn sie eine kleine Zahl Passwörter im Wechsel verwenden können, wird die Effektivität einer guten Passwortrichtlinie deutlich reduziert.

Wenn diese Einstellung auf einen kleinen Wert gesetzt wird, sind die Benutzer in der Lage, eine kleine Zahl von Passwörtern immer wieder zu verwenden. Wenn die Einstellung **Minimales Passwortalter** nicht zusätzliche definiert ist, sind die Benutzer in der Lage, das Passwort mehrmals hintereinander zu ändern. Sie können so das alte Passwort sofort wieder verwenden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf den Maximalwert von **24**. Damit sie eine Wirkung zeigt, sollten Sie die Einstellung **Minimales Passwortalter** ebenfalls konfigurieren. Dieser Wert sollte mit der Einstellung **Maximales Passwortalter** und dem Änderungsintervall für die Passwörter abgestimmt werden.

Mögliche Auswirkungen

Die Benutzer müssen bei jeder Passwortänderung ein neues Passwort verwenden. Das Risiko, dass die Benutzer anfangen die Passwörter aufzuschreiben, steigt.

Maximales Passwortalter

Die Einstellung legt die Anzahl von Tagen fest, die ein Passwort verwendet werden kann, bevor es geändert werden muss.

Die möglichen Werte sind:

- **Ein benutzerdefinierter Wert zwischen 0 und 999**
- **Nicht konfiguriert**

Sicherheitslücken

Jedes Passwort kann geknackt werden. Mit momentaner Computerleistung ist selbst das Entschlüsseln des komplexesten Passworts nur eine Frage von Zeit und Prozessorleistung. Einige der folgenden Einstellungen können die Möglichkeit, ein Passwort in einer vertretbaren Zeit zu knacken, verringern. Das regelmäßige Ändern der Benutzerpasswörter Ihrer Umgebung reduziert das Risiko, dass ein gültiges Passwort geknackt, oder ein Passwort missbraucht wird. Das maximale Passwortalter kann so konfiguriert werden, dass die Benutzer ihr Passwort nie ändern müssen. Dies würde allerdings ein großes Sicherheitsrisiko darstellen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **30** bis **40** Tage. Wenn Sie den Wert auf **Null** setzten, laufen die Passwörter niemals ab.

Mögliche Auswirkungen

Wenn Sie die Einstellung auf einen zu kleinen Wert setzen, müssen die Benutzer ihr Passwort sehr häufig ändern. Dies könnte die Sicherheit sogar verschlechtern, da die Benutzer ihre Passwörter dann möglicherweise aufschreiben. Wenn Sie den Wert zu hoch setzen, hat ein potentieller Angreifer mehr Zeit Passwörter zu knacken. Dies verschlechtert die Sicherheit ebenfalls.

Minimales Passwortalter

Diese Einstellung legt die Anzahl an Tagen fest, die ein Passwort verwendet werden muss, bevor es geändert werden kann. Sie muss unter dem Wert der Einstellung **Maximales Passwortalter** liegen. Die Einstellung **Passwortchronik erzwingen** ist nur aktiv, wenn diese Einstellung auf einen Wert größer Null konfiguriert ist.

Die möglichen Werte sind:

- **Ein benutzerdefinierter Wert zwischen 0 und 998**
- **Nicht konfiguriert**

Sicherheitslücken

Es ist nutzlos, die Benutzer zur regelmäßigen Änderung ihrer Passwörter zu zwingen, wenn diese einfach alle gespeicherten Passwörter der Passwortchronik durchgehen können, bis sie das alte Passwort wieder haben. Mit dieser Einstellung und der Einstellung **Passwortchronik erzwingen** verhindern Sie dies.

Gegenmaßnahmen

Setzten Sie den Wert der Einstellung auf **zwei Tage.** Wenn der Wert auf Null konfiguriert ist, kann das Passwort sofort wieder geändert werden, was natürlich nicht empfehlenswert ist.

Mögliche Auswirkungen

Es gibt eine wichtige Auswirkung dieser Einstellung: Wenn der Administrator das Passwort eines Benutzers ändert, und der Benutzer dieses dann sofort in ein eigenes Passwort ändern soll, dann muss der Administrator das Kontrollkästchen **Benutzer muss Passwort bei der nächsten Anmeldung ändern** aktivieren. Ansonsten ist dieser nicht in der Lage sein Passwort sofort zu ändern.

Minimale Passwortlänge

Diese Einstellung legt fest, aus wie vielen Zeichen das Passwort eines Benutzerkontos mindestens bestehen muss. Es gibt zur bestmöglichen Passwortlänge viele unterschiedliche Meinungen. Eine Passphrase ist aber zum Beispiel definitiv besser als „password“. Unter Windows 2000 und den nachfolgenden Versionen können Passphrasen sehr lang werden und Leerzeichen enthalten. Daher ist "Ich möchte einen 5€ Milchshake trinken " zum Beispiel eine gültige Passphrase. Sie ist besser als eine acht oder zehn Zeichen lange Zeichenkette, und sie ist einfacher zu merken.

Die möglichen Werte sind:

- **Ein benutzerdefinierter Wert zwischen 0 und 14**
- **Nicht konfiguriert**

Sicherheitslücken

Es gibt einige unterschiedliche Arten von Passwortangriffen die verwendet werden können, um das Passwort eines Benutzerkontos zu erlangen. Zum Beispiel Wörterbuchangriffe, bei denen gebräuchliche Wörter verwendet werden, oder Brute-Force-Angriffe, die einfach jede mögliche Passwortkombination ausprobieren. Ein Angriff könnte auch auf die Kontendatenbank abzielen und Tools zum Knacken der Konten und Passwörter verwenden.

Gegenmaßnahmen

Setzen Sie den Wert auf mindestens acht. Wenn er auf null konfiguriert ist, ist kein Passwort erforderlich. Für die meisten Umgebungen wird eine Passwortlänge von acht Zeichen empfohlen. Dies ist für eine entsprechende Sicherheit genug, jedoch immer noch so kurz, dass die Benutzer sich das Passwort merken können. Diese Einstellung bietet einen Schutz gegen Brute-Force-Angriffe. Wenn die Komplexitätsanforderungen zusätzlich durchgesetzt werden, erhöht dies den Schutz vor Wörterbuchangriffen. Diese werden im nächsten Abschnitt besprochen.

Mögliche Auswirkungen

Wenn kurze Passwörter möglich sind, verringert dies die Sicherheit. Solche Passwörter können über einen Wörterbuch- oder Brute-Force-Angriff sehr einfach geknackt werden. Sehr lange Passwörter könnten zu Falscheingaben und so zu einer höheren Belastung des Benutzer-Helpdesks führen. Außerdem kann sich die Sicherheit der Organisation verschlechtern, da die Benutzer die Passwörter aufschreiben, um sie sich zu merken. Dies kann durch die Verwendung von Passphrasen verhindert werden.

Passwörter müssen Komplexitätsvoraussetzungen entsprechen

Diese Einstellung legt fest, ob die Passwörter einigen Richtlinien für starke Passwörter entsprechen müssen.

Wenn Sie aktiviert ist, müssen die Passwörter den folgenden Vorgaben entsprechen:

- Das Passwort darf nicht mit dem Benutzernamen übereinstimmen, oder Teile von diesem enthalten.
- Das Passwort ist mindestens sechs Zeichen lang.
- Das Passwort enthält Zeichen aus den folgenden Kategorien:
    - Großbuchstaben (A-Z)
    - Kleinbuchstaben (a-z)
    - Zahlen (0-9)
    - Sonderzeichen (zum Beispiel !, $, # oder %)

Diese Anforderungen werden bei der Änderung oder Neuanlage eines Passwortes durchgesetzt. Sie können nicht direkt verändert werden. Es ist allerdings möglich, über eine neue Version der Datei *passfilt.dll* andere Regeln durchzusetzen. Den Quellcode der Datei *passfilt.dll* finden Sie im Microsoft Knowledge Base Artikel 151082: *HOW TO: Password Change Filtering & Notification in Windows NT*. (englischsprachig)

Die möglichen Werte für die Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Passwörter, die nur aus alphanumerischen Zeichen bestehen, sind extrem einfach zu knacken. Werkzeuge hierzu sind öffentlich verfügbar. Um dies zu verhindern, sollten die Komplexitätsanforderungen durchgesetzt werden.

Gegenmaßnahmen

Setzten Sie die Einstellung auf **Aktiviert**. Kombiniert mit der Einstellung **Minimale Passwortlänge** auf **8** sind so mindestens 218.340.105.584.896 unterschiedliche Passwörter möglich. Dies macht einen Brute-Force-Angriff schwer, aber nicht unmöglich. Ein Angreifer, der über genug Rechenzeit verfügt um eine Millionen Passwörter pro Sekunde zu testen, könnte ein solches Passwort in weniger als sieben Tagen herausfinden.

Mögliche Auswirkungen

Bei der Verwendung der Standard-*passfilt.dll* könnte es zu zusätzlichen Anfragen beim Benutzerhelpdesk kommen. Zum Beispiel, weil die Benutzer es nicht gewohnt sind, Sonderzeichen zu verwenden. Die Einstellung ist jedoch großzügig genug, damit alle Benutzer in der Lage sein sollten, die Anforderungen recht schnell zu erlernen. Eine zusätzliche Einstellung, die über die Datei passfilt.dll durchgesetzt werden könnte, wäre zum Beispiel die Verwendung von Zeichen, die über die ALT-Taste erreichbar sind. Die Durchsetzung solcher Vorgaben kann allerdings schnell zu sehr schlecht gelaunten Benutzern und einem ausgelasteten Benutzerhelpdesk führen. Sie könnten die Verwendung von ALT-Zeichen zwischen 0128 und 0159 für die Administratorkonten durchsetzten. Die Verwendung anderer ALT-Zeichen hat keine Wirkung, da diese normale alphanumerische Zeichen repräsentieren.

Kennwörter für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern

Diese Einstellung legt fest, ob Windows Server 2003, Windows 2000 Server, Windows 2000 Professional und Windows XP Professional Passwörter mit umkehrbarer Verschlüsselung speichern. Sie unterstützt Anwendungen, die Protokolle verwenden, welche darauf angewiesen sind, zur Authentifizierung das Benutzerpasswort zu kennen. Ein Angreifer, der in der Lage ist die Verschlüsselung zu knacken, könnte mit dem so kompromittieren Konto auf Netzwerkressourcen zugreifen. Aus diesem Grund sollten Sie diese Einstellung niemals aktivieren. Es sei den, der Nutzen von Anwendungen, die dies erfordern, überwiegt in Ihrer Umgebung den Schutz der Passwörter.

Für die Verwendung von CHAP für einen RAS-Zugriff, einen IAS-Zugriff (Internet Authentication Service) oder für die Digest-Authentifizierung der IIS (Internet Information Services) muss diese Einstellung aktiviert sein.

Die möglichen Werte sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Die Einstellung bewirkt, dass Windows Server 2003 Passwörter in einem schwächeren Format speichert. Dieses ist anfälliger für Brute-Force-Angriffe.

Gegenmaßnahmen

Setzen Sie den Wert der Einstellung auf **Deaktiviert.**

Mögliche Auswirkungen

Die Verwendung des CHAP Authentifizierungsprotokolls für RAS oder IAS und die Digest-Authentifizierung der IIS ist nur möglich, wenn die Einstellung **Deaktiviert** ist. Dies ist jedoch sehr gefährlich.

> **Warnung: Aktivieren Sie diese Einstellung niemals.** Es sei denn, zwingende geschäftliche Anforderungen überwiegen die Risiken.

Kontosperrungsrichtlinien

Wenn es zu mehr als ein paar fehlgeschlagenen Anmeldeversuchen kommt, könnte das auf einen Angreifer hindeuten, der versucht ein Kontopasswort zu erraten. Windows Server 2003 protokolliert Anmeldeversuche. Das Betriebssystem kann so konfiguriert werden, dass es auf solche Angriffe mit einer zeitweisen Sperrung des Kontos reagiert. Die Kontosperrungsrichtlinien legen die Grenzwerte hierfür fest. In der Excel-Tabelle *Windows Standardeinstellungen für Sicherheit und Dienste,* die Sie zusammen mit diesem Handbuch erhalten haben, werden die Standardeinstellungen beschrieben. Sie finden die Kontosperrungsrichtlinien im Gruppenrichtlinieneditor unter dem folgenden Pfad: *Computerkonfiguration\Windows Einstellungen\Sicherheitseinstellungen\Kontenrichtlinien\Kontosperrungsrichtlinie*

Kontosperrdauer

Diese Einstellung legt die Dauer in Minuten fest, für die ein Konto gesperrt bleibt, bevor es automatisch entsperrt wird. Wenn Sie den Wert auf N**ull** konfigurieren, dann bleibt das Konto gesperrt, bis ein Administrator es manuell entsperrt. Die Einstellung muss auf einen Wert größer oder gleich der Einstellung **Zurücksetzungsdauer des Kontosperrungszählers** konfiguriert sein.

Die möglichen Werte sind:

- **Ein benutzerdefinierter Wert in Minuten zwischen 0 und 99.999**
- **Nicht konfiguriert**

Sicherheitslücken

Ein DoS-Angriff (Denial of Service) könnte durchgeführt werden, indem ein Angreifer einfach mit ungültigen Anmeldungen die **Kontensperrungsschwelle** überschreitet. Wenn diese konfiguriert ist, wird das Konto nach einer definierten Zahl von ungültigen Anmeldeversuchen gesperrt. Wenn dann die Einstellung **Kontosperrdauer** auf Null gesetzt ist, bleibt das Konto bis zur Entsperrung durch den Administrator gesperrt.

Gegenmaßnahmen

Setzen Sie den Wert der Einstellung auf **30 Minuten**.

Mögliche Auswirkungen

Obwohl es eine gute Idee zu sein scheint, die Einstellung so zu konfigurieren, dass ein Konto niemals automatisch entsperrt wird, kann die Zahl der Anfragen durch versehendlich gesperrte Konten beim Benutzerhelpdesk deutlich steigen.

Kontensperrungsschwelle

Diese Einstellung legt die Zahl der fehlgeschlagenen Anmeldeversuche fest, die zu einer Kontosperrung führen. Dieses Konto kann bis zur automatischen Entsperrung oder der Entsperrung durch einen Administrator nicht mehr verwendet werden. Wenn Sie für diese Einstellung den Wert Null konfigurieren, wird das Konto niemals gesperrt.

Fehlgeschlagene Versuche auf Arbeitsstationen, die durch STRG+ALT+ENTFERNEN oder durch den Bildschirmschoner gesperrt wurden, werden nur mitgezählt, wenn die Einstellung **Interaktive Anmeldung: Domänencontrollerauthentifizierung zum Aufheben der Sperrung der Arbeitsstation erforderlich** aktiviert wurde.

Die möglichen Werte sind:

- **Ein benutzerdefinierter Wert zwischen 0 und 999**
- **Nicht konfiguriert**

Sicherheitslücken

Passwortangriffe können über eine automatische Verarbeitung Tausende oder auch Millionen von Passwortkombinationen durchgehen. Wenn die Zahl der möglichen Anmeldeversuche eingeschränkt wird, werden solche Angriffe nahezu beseitigt. Es ist allerdings möglich, dass mit dieser Einstellung ein DoS-Angriff gegen die entsprechende Domäne durchgeführt werden kann. Ein Angreifer könnte über ein automatisches Verfahren für alle Benutzer der Domäne falsche Anmeldeversuche durchführen. Wenn die Zahl der Versuche die Kontosperrungsschwelle übersteigt, werden diese Konten alle gesperrt.

Gegenmaßnahmen

Da durch eine Aktivierung und durch eine Deaktivierung dieser Einstellung Nachteile entstehen können, gibt es zwei mögliche Gegenmaßnahmen. Eine Organisation muss zwischen den beiden Möglichkeiten und den daraus entstehenden Risiken abwägen.

- Die **Kontensperrungsschwelle** auf **Null** setzen – Dies stellt sicher, dass keine Konten gesperrt werden. Ein DoS-Angriff wird so vermieden. Anfragen beim Benutzerhelpdesk wegen versehentlich gesperrter Konten gibt es nicht.
  Ein Brute-Force-Angriff wird jedoch nicht verhindert. Daher sollte diese Konfiguration nur gewählt werden, wenn die folgenden beiden Kriterien zutreffen:
  - Die Passwortrichtlinie erzwingt für alle Benutzer komplexe Passwörter mit acht oder mehr Zeichen.
  - Es gibt einen zuverlässigen Überwachungsmechanismus, der die Administratoren bei einer größeren Zahl von fehlgeschlagenen Anmeldeversuchen benachrichtigt.
- Wenn diese Kriterien nicht eingehalten werden können, setzen Sie die Einstellung **Kontensperrungsschwelle** auf einen Wert, der so hoch gewählt ist, dass eine versehentliche Fehleingabe eines Benutzers nicht sofort zur einer Kontosperrung führt, jedoch ein Brute-Force-Passwortangriff verhindert wird. Ein Wert von 50 fehlgeschlagenen Versuchen sollte ein guter Kompromiss sein.

Mögliche Auswirkungen

Die Aktivierung dieser Einstellung verhindert die Verwendung von gesperrten Konten. Sie wird wahrscheinlich zu einer leichten Steigerung der Anfragen beim Benutzerhelpdesk führen. Tatsächlich machen in manchen Organisationen die Anfragen wegen gesperrter Konten den größten Teil aller Anfragen aus.

Wenn der Wert der Einstellung auf Null konfiguriert ist, ist es möglich, dass ein Angreifer bei einem Brute-Force-Angriff unentdeckt bleibt.

Zurücksetzungsdauer des Kontosperrungszählers

Diese Einstellung legt die Dauer in Minuten fest, nach welcher der Zähler für fehlgeschlagene Anmeldungen auf Null zurückgesetzt wird. Wenn die Einstellung **Kontensperrungsschwelle** definiert ist, muss der Wert dieser Einstellung kleiner oder gleich der **Kontosperrungsdauer** sein.

- **Ein benutzerdefinierter Wert zwischen 1 und 99.999.**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten das eigene Konto versehendlich durch mehrfache Fehleingabe des Passwortes sperren.

Gegenmaßnahmen

Setzen Sie die Einstellung auf einen Wert von **30 Minuten**.

Mögliche Auswirkungen

Wenn die Einstellung nicht oder zu hoch konfiguriert ist, könnte dies zu einem DoS-Angriff führen. Ein Angreifer könnte einige falsche Anmeldeversuche durchführen und so Konten sperren. Wenn diese Einstellung nicht konfiguriert ist, muss der Administrator in diesem Fall das Konto manuell entsperren.

Kerberos-Richtlinien

Unter Windows Server 2003 stellt das Authentifizierungsprotokoll Kerberos Version 5 die Standardmechanismen für die Authentifizierung und die benötigten Autorisationsdaten zur Verfügung. In dem die Lebensdauer von Kerberos-Tickets verringert wird, kann das Risiko verringert werden, dass ein Angreifer die gestohlenen Authentifizierungsdaten eines Benutzers für einen Zugriff verwendet. Der Autorisationsaufwand steigt allerdings. In den meisten Umgebungen sollten diese Einstellungen nicht geändert werden. Sie werden auf Domänenebene angewandt, und in der *Default Domain Policy* einer Windows 2000- oder Windows Server 2003-Domäne sind bereits Standardwerte definiert. In der Excel-Tabelle *Windows Standardeinstellungen für Sicherheit und Dienste,* die Sie mit diesem Handbuch erhalten haben, werden die Standardeinstellungen beschrieben.

Sie können die Einstellungen der Kerberos Richtlinie im Gruppenrichtlinieneditor über den folgenden Pfad bearbeiten:
Computerkonfiguration\Windows Einstellungen\Sicherheitseinstellungen\Kontorichtlinien\Kerberos Richtlinie

Benutzeranmeldeeinschränkungen erzwingen

Diese Einstellung legt fest, ob jede Anfrage für ein Sitzungsticket vom Kerberos V5 Key Distribution Center (KDC) gegen die Benutzerrechte des Kontos geprüft wird. Dieser zusätzliche Schritt erfordert zusätzlichen Aufwand, und er könnte den Netzwerkzugriff auf Dienste verlangsamen.

Die möglichen Werte sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn die Einstellung deaktiviert ist, könnten Benutzer ein Sitzungsticket für einen Dienst erhalten, den sie nicht verwenden dürfen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Keine, da es sich um die Standardeinstellung handelt.

Maximale Gültigkeitsdauer des Diensttickets

Diese Sicherheitseinstellung legt die Zeitspanne (in Minuten) fest, den ein Sitzungsticket zum Zugriff auf einen Dienst verwendet kann. Sie muss auf zehn Minuten oder größer konfiguriert sein, und sie darf nicht größer als die Einstellungen **Max. Gültigkeitsdauer des Benutzertickets** sein. Wenn ein Client mit einem abgelaufenen Ticket versucht auf einen Server zuzugreifen, antwortet dieser mit einer Fehlermeldung. Der Client muss dann ein neues Sitzungsticket beim Kerberos V5 Key Distribution Center (KDC) anfordern. Sobald eine Verbindung authentifiziert ist, ist es egal, wie lange das Sitzungsticket noch gültig ist. Wenn es abläuft, werden die bestehenden Verbindungen hiervon nicht beeinflusst.

Die möglichen Werte sind:

- **Ein benutzerdefinierter Zeitraum in Minuten zwischen 10 und 99.999, in dem das Ticket gültig bleibt.**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn der Wert dieser Einstellung zu hoch gewählt wurde, könnten Benutzer in der Lage sein, außerhalb ihrer Anmeldezeiten auf Netzwerkressourcen zuzugreifen. Es könnte auch sein, dass Benutzer mit deaktivierten Konten trotzdem auf das Netzwerk zugreifen können, da sie ein gültiges Dienstticket schon vor der Deaktivierung ihres Kontos erhalten haben und dieses zu lange gültig bleibt.

Gegenmaßnahmen

Setzen Sie den Wert der Einstellung auf **600 Minuten**.

Mögliche Auswirkungen

Keine, da es sich um die Standardeinstellungen handelt.

Maximale Gültigkeitsdauer des Benutzertickets

Diese Einstellung legt den maximalen Zeitraum (in Stunden) fest, den das Ticket Granting Ticket (TGT) eines Benutzers gültig bleibt. Wenn das TGT abläuft, muss ein neues angefordert, oder das alte erneuert werden.

Die möglichen Werte sind:

- **Ein benutzerdefinierter Wert in Stunden zwischen 0 und 99.999**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn der Wert dieser Einstellung zu hoch gewählt wurde, könnten Benutzer in der Lage sein außerhalb ihrer Anmeldezeiten auf Netzwerkressourcen zuzugreifen. Es könnte auch sein, dass Benutzer mit deaktivierten Konten trotzdem auf das Netzwerk zugreifen können, da sie ein gültiges Dienstticket schon vor der Deaktivierung ihres Kontos erhalten haben und dieses zu lange gültig bleibt.

Gegenmaßnahmen

Setzen Sie den Wert dieser Einstellung auf **10 Stunden**.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Maximaler Zeitraum, in dem ein Benutzerticket erneuert werden kann

Diese Einstellung legt den Zeitraum fest, in dem ein Ticket Granting Ticket (TGT) erneuert werden kann.

Die möglichen Werte sind:

- **Ein benutzerdefinierter Zeitraum in Minuten zwischen 10 und 99.999.**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn der Wert der Einstellung zu hoch gewählt wurde, können sehr alte Tickets erneuert werden.

Gegenmaßnahmen

Setzen Sie den Wert der Einstellung auf **sieben Tage**.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Maximale Toleranz für die Synchronisation des Computertakts

Diese Einstellung legt die maximale Abweichung der Uhrzeiten zwischen Client und Domänencontroller fest, die Kerberos V5 toleriert.

Die möglichen Werte sind:

- **Ein benutzerdefinierter Zeitraum in Minuten zwischen 1 und 99.999.**
- **Nicht konfiguriert**

Sicherheitslücken

Um Replay-Angriff zu verhindern, verwendet Kerberos V5 Zeitstempel. Damit diese Zeitstempel korrekt funktionieren, müssen die Uhren der Domänencontroller und der Clients so synchron wie möglich laufen. Da die Uhren zweier verschiedener Computer jedoch oft asynchron sind, können Administratoren über diese Einstellung eine maximale Abweichung festlegen. Wenn der Zeitstempel eines Tickets um einen größeren Wert als den der Einstellung abweicht, so wird dieses nicht akzeptiert.

Gegenmaßnahmen

Setzen Sie den Wert der Einstellung auf **fünf Minuten**.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

3
Überwachungsrichtlinien

Das Überwachungsprotokoll erzeugt bei bestimmten, vordefinierten, Benutzeraktionen einen Eintrag. Dies könnte zum Beispiel das Ändern einer Datei oder einer Richtlinie sein. Der Überwachungseintrag informiert Sie über die durchgeführte Aktion, das verwendete Benutzerkonto und über Datum und Uhrzeit der Aktion. Sie können sowohl erfolgreiche, als auch fehlgeschlagene Aktionen überwachen lassen.

Betriebssysteme und Anwendungen sind „dynamisch“. Das heißt, es könnte zum Beispiel kurzfristig notwendig sein, eine Sicherheitseinstellung zeitweise zu ändern, um eine bestimmte Aktion durchführen zu können. Häufig wird dann jedoch vergessen, diese Einstellung rückgängig zu machen. Das würde bedeuten, dass der Computer möglicherweise den Sicherheitsanforderungen des Unternehmens nicht mehr entspricht.

Eine regelmäßige Analyse ermöglicht es einem Administrator, für alle Computer eine ausreichende Sicherheit zu gewährleisten. Solche Analysen konzentrieren sich auf sehr spezielle Informationen, und sie können so zur Erkennung von Sicherheitsproblemen beitragen.

Da die Überwachungsprotokolle möglicherweise der einzige Indikator für einen Sicherheitsbruch sein könnten, spielen Sie für jedes Unternehmen eine wichtige Rolle. Wenn das Sicherheitsproblem erkannt wurde, können die Protokolle außerdem wertvolle zusätzliche Informationen enthalten.

Protokolle für fehlgeschlagene Aktionen sind oft informativer als solche für erfolgreiche Aktionen, da Fehlschläge typischerweise auf Fehler hinweisen. Wenn ein Benutzer sich zum Beispiel erfolgreich an einem System anmeldet, dann wird dies als normal betrachtet. Wenn ein Benutzer sich allerdings mehrmals erfolglos anzumelden versucht, kann dies darauf hinweisen, dass jemand versucht, in das System einzubrechen. Über die Überwachungsrichtlinie werden Einstellungen, wie die maximale Protokollgröße, die Zugriffsrechte auf die Protokolle und deren Aufbewahrungsdauer und –methode festgelegt. Die Standardeinstellungen finden Sie, wie immer, in der Excel-Tabelle.

Sie können im Gruppenrichtlinieneditor über den folgenden Pfad auf die Überwachungsrichtlinie zugreifen:
Computerkonfiguration\Windows Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Überwachungsrichtlinie

Überwachungseinstellungen

Die Sicherheitslücken, Gegenmaßnahmen und möglichen Auswirkungen aller Überwachungseinstellungen sind identisch. Daher werden diese nur einmal im folgenden Absatz beschrieben. Dann folgen genaue Beschreibungen der einzelnen Einstellungen.

Die Möglichen Werte aller Überwachungseinstellungen sind:

- **Erfolgreich**
- **Fehlgeschlagen**
- **Keine Überwachung**

Sicherheitslücken

Wenn keine Überwachung konfiguriert ist, wird es schwer oder unmöglich festzustellen, was während

eines Sicherheitsvorfalles passiert ist. Wenn die Überwachung allerdings so konfiguriert wurde, dass zu viele Einträge produziert werden, dann wird das Protokoll mit nutzlosen Daten gefüllt und die Gesamtleistung des Systems könnte sich verschlechtern.

Gegenmaßnahmen

Auf allen Computern Ihrer Organisation sollten passende Überwachungsrichtlinien definiert sein, so dass die Aktivitäten der berechtigten Benutzer ignoriert, und die der unautorisierten Benutzer aufgezeichnet werden.

Mögliche Auswirkungen

Wenn keine Überwachung konfiguriert wurde, oder diese zu gering ist, wird es für eine Analyse nach einem Sicherheitsvorfall entweder keine oder mangelhafte Beweise geben. Wenn die Überwachung andererseits zu umfangreich ist, füllt sich das Protokoll mit bedeutungslosen Einträgen.

Anmeldeversuche überwachen

Diese Einstellung legt fest, ob die An- und Abmeldeversuche überwacht werden. Sie können sowohl die erfolgreichen, als auch die fehlgeschlagenen Versuche überwachen. Wenn die Überwachung auf einem Domänencontroller definiert wurde, wird für jeden Benutzer, der gegen diesen eine Authentifizierung durchführt, ein Eintrag erzeugt. Dies passiert auch dann, wenn der Benutzer in diesem Moment an einer Arbeitsstation angemeldet ist, die Mitglied der Domäne ist.

Kontenverwaltung überwachen

Diese Einstellung legt fest, ob auf einem Computer die Verwaltung von Konten überwacht wird. Beispiele für die Kontenverwaltung sind unter anderem:

- Ein Benutzerkonto oder eine Gruppe wird erstellt, geändert oder gelöscht.
- Ein Benutzerkonto wird umbenannt, deaktiviert oder aktiviert.
- Ein Passwort wird gesetzt oder geändert.

Sie können natürlich wieder eine Erfolgs- oder Fehlerüberwachung konfigurieren. Die Erfolgsüberwachung sollte auf allen Computer des Unternehmens konfiguriert sein. Bei der Verfolgung von Sicherheitsvorfällen ist es lebensnotwendig, dass festgestellt werden kann, wer ein Konto erstellt, geändert oder gelöscht hat.

Verzeichniszugriff überwachen

Diese Einstellung überwacht den Zugriff auf Microsoft® Active Directory® Objekte, für die eine System Access Control List (SACL - Zugriffskontrollliste) definiert wurde. Eine SACL definiert eine Liste von Benutzern und Gruppen, für die Aktionen überwacht werden. Die Aktivierung dieser Einstellung kann auf Domänencontrollern eine große Zahl an Einträgen produzieren. Sie sollten dies daher nur machen, wenn Sie solche Informationen benötigen.

Eine SACL können Sie über die Registerkarte **Sicherheit** im Eigenschaftsfenster eines Active Directory-Objektes definieren.

Anmeldeereignisse überwachen

Diese Einstellung legt fest, ob die An- und Abmeldeversuche überwacht werden. Sie können sowohl

die erfolgreichen, als auch die fehlgeschlagenen Versuche überwachen. Wenn die Überwachung auf einem Domänencontroller definiert wurde, wird für Benutzer, die sich an einer Arbeitsstation anmelden, kein Eintrag erzeugt. Nur interaktive Anmeldungen und Netzwerkanmeldungen generieren ein Ereignis.

Objektzugriff überwachen

Diese Einstellung überwacht den Zugriff auf Objekte. Objekte sind zum Beispiel Dateien, Ordner, Registrierungsschlüssel und Drucker für die eine System Access Control List (SACL - Zugriffskontrollliste) definiert wurde. Eine SACL definiert eine Liste von Benutzern und Gruppen, für die Aktionen überwacht werden. Die Aktivierung dieser Einstellung kann auf Domänencontrollern eine große Zahl an Einträgen produzieren. Sie sollten dies daher nur vornehmen, wenn Sie diese Informationen benötigen. Eine Fehlerüberwachung könnte bei dieser Einstellung unerwartet viele Einträge erzeugen. Das liegt daran, dass zum Beispiel viele Anwendungen erst versuchen, Dateien mit Lese- und Schreibberechtigung zu öffnen. Wenn das nicht funktioniert, dann öffnen sie die Datei einfach mit Leseberechtigung. In diesem Fall würde eine Fehlerüberwachung - bei einer entsprechend konfigurierten SACL - schon einen Eintrag generieren.

Anmerkung: Das Aktivieren einer Überwachung eines Objektes, wie zum Beispiel einer Datei, eines Ordners oder eines Druckers, besteht aus zwei Schritten. Nach der Aktivierung der Richtlinie müssen Sie die SACLs der entsprechenden Objekte anpassen. Wenn Sie zum Beispiel die Zugriffsversuche der Benutzer auf eine bestimmte Datei überwachen möchten, müssen Sie die entsprechenden Attribute über die Sicherheitseinstellungen der Datei bearbeiten.

Richtlinienänderung überwachen

Diese Einstellung legt fest, welche Änderungen an Benutzerrechten und Überwachungsrichtlinien protokolliert werden.

Rechteverwendung überwachen

Dieses Recht legt fest, ob die Verwendung von Benutzerrechten überwacht wird. Bei einer Aktivierung dieser Einstellungen wird eine große Zahl von Einträgen erzeugt. Sie sollten dies nur machen, wenn Sie diese Informationen benötigen. Die folgenden Benutzerrechte werden nicht überwacht:

- Auslassen der durchsuchenden Überprüfung
- Erstellen eines Token-Objektes
- Ersetzen eines Tokens auf Prozessebene
- Sicherheitsüberwachung generieren
- Dateien und Verzeichnisse sichern
- Dateien und Verzeichnisse wiederherstellen

Prozessverfolgung überwachen

Diese Einstellung legt fest, ob detaillierte Aktionen, wie zum Beispiel die Aktivierung eines Programms, das Beenden eines Prozesses, eine Handelduplizierung oder ein indirekter Objektzugriff überwacht werden.

Bei einer Aktivierung dieser Einstellungen wird eine große Zahl von Einträgen erzeugt. Sie sollten dies nur machen, wenn Sie solche Informationen benötigen. Bei einem Sicherheitsvorfall können die Informationen allerdings von großem Nutzen sein. Sie können dann zum Beispiel feststellen, welche Prozesse wann und wie gestartet wurden.

Systemereignisse überwachen

Diese Überwachung erzeugt unter anderem Einträge, wenn ein Benutzer ein System neu startet oder herunterfährt, oder wenn ein Ereignis auftritt, dass die Systemsicherheit oder das Sicherheitsprotokoll betrifft. Da die erzeugten Einträge der Erfolgsüberwachung und der Fehlerüberwachung sehr wichtig sind, sollten Sie die Einstellung auf allen Computern Ihrer Organisation aktivieren.

Überwachungsbeispiel: Ergebnisse einer Benutzeranmeldung

Nachdem Sie nun die unter Windows verfügbaren Überwachungseinstellungen kennen, wollen wir Ihnen ein Überwachungsbeispiel zeigen. Ereignisse werden jeweils auf den einzelnen Systemen protokolliert. Um festzustellen was passiert ist, könnte es sein, dass Sie die Sicherheitsprotokolle mehrerer Systeme prüfen und deren Daten zusammenfassen müssen.

Der Rest dieses Kapitels beschreibt die Kernereignisse, die bei der Anmeldung eines Benutzers an einen Computer und einem darauf folgenden Zugriff dieses Benutzers auf eine Freigabe eines Dateiservers, in das Ereignisprotokoll des Domänencontrollers, Dateiservers und der Arbeitsstation geschrieben werden. Nur die wichtigsten Ereignisse werden beschrieben. Alle anderen Ereignisse wurden aus Gründen der Übersichtlichkeit weggelassen.

Die Namen der Konten und Ressourcen, die in diesem Beispiel verwendet werden:

- Domäne = DOM
- Domänencontroller = DC1
- Dateiserver = FS1
- Arbeitsstation des Benutzers = XP1
- Benutzer = John
- Freigabe auf FS1 = Share
- Datei in der Freigabe = document.txt

Benutzer meldet sich an seinem Computer an

- Ereignisse, die auf der Arbeitsstation aufgezeichnet werden
  - Erfolgsüberwachung für Ereignis ID 528, Benutzer-Anmeldung/Abmeldung für Benutzer DOM\John auf Maschine XP1
- Ereignisse auf dem Domänencontroller
  - Erfolgsüberwachung für Ereignis ID 540, Benutzer-Anmeldung/Abmeldung für Benutzer DOM\John auf Maschine DC1
- Ereignisse auf dem Dateiserver
  - Keine

Benutzer greift auf die Freigabe „Share“ zu

- Ereignisse, die auf der Arbeitsstation aufgezeichnet werden
  - Keine
- Ereignisse auf dem Domänencontroller

    - Erfolgsüberwachung für Ereignis ID 673, Kontoanmeldung für Benutzer John@DOM.com für Dienstname FS1$
    - Erfolgsüberwachung für Ereignis ID 673, Kontoanmeldung für Benutzer FS$@DOM.com für Dienstname FS1$
    - Erfolgsüberwachung für Ereignis ID 673, Kontoanmeldung für Benutzer XP1$@DOM.com für Dienstname FS1$

    Anmerkung: Dies sind alles Kerberos-Ticketanfragen

- Ereignisse auf dem Dateiserver
    - Erfolgsüberwachung für Ereignis ID 540, Benutzer Anmeldung/Abmeldung für Benutzer DOM\John auf Maschine FS1
    - Erfolgsüberwachung für Ereignis ID 560, Objektzugriff für Benutzer DOM\John auf das Objekt C:\Share mit Zugriffstyp READ_CONTROL, ReadData (oder ListDirectory), ReadEA und ReadAttributes
    - Erfolgsüberwachung für Ereignis ID 560, Objektzugriff für Benutzer DOM\John auf das Objekt C:\Share\document.txt mit Zugriffstyp READ_CONTROL, ReadData (oder ListDirectory), ReadEA und ReadAttributes

Benutzer öffnet die Datei document.txt

- Ereignisse, die auf der Arbeitsstation aufgezeichnet werden
    - Keine
- Ereignisse auf dem Domänencontroller
    - Keine
- Ereignisse auf dem Dateiserver
    - Erfolgsüberwachung für Ereignis ID 560, Objektzugriff für Benutzer DOM\John auf das Objekt C:\Share\document.txt mit Zugriffstyp READ_CONTROL, ReadData (oder ListDirectory), WriteDate (oder AddFile), AppendDate (oder AddSubdirectory oder CreatePipeInstance), ReadEA, WriteEA, ReadAttributes und WriteAttributes
    - Erfolgsüberwachung für Ereignis ID 560, Objektzugriff für Benutzer DOM\John auf das Objekt C:\Share mit Zugriffstyp ReadAttributes
    - Erfolgsüberwachung für Ereignis ID 560, Objektzugriff für Benutzer DOM\John auf das Objekt C:\Share\document.txt mit Zugriffstyp ReadAttributes

Benutzer speichert die Datei document.txt

- Ereignisse, die auf der Arbeitsstation aufgezeichnet werden
    - Keine
- Ereignisse auf dem Domänencontroller
    - Keine
- Ereignisse auf dem Dateiserver
    - Erfolgsüberwachung für Ereignis ID 560, Objektzugriff für Benutzer DOM\John auf das Objekt C:\Share\document.txt mit Zugriffstyp SYNCHRONIZE, ReadData (oder ListDirectory), WriteDate (oder AddFile), AppendDate (oder AddSubdirectory oder CreatePipeInstance), ReadEA, WriteEA, ReadAttributes und WriteAttributes

- Erfolgsüberwachung für Ereignis ID 560, Objektzugriff für Benutzer DOM\John auf das Objekt C:\Share\document.txt mit Zugriffstyp READ_CONTROL, SYNCHRONIZE und ReadData (oder ListDirectory)

Dieses Beispiel scheint, obwohl es bereits vereinfacht wurde, sehr komplex. Die oben beschriebenen Schritte würden in Wirklichkeit ein Dutzend Anmelde-, Abmelde- und Rechteverwendungsereignisse erzeugen. Wenn der Benutzer eine Datei öffnet, werden außerdem Objektzugriffsereignisse erzeugt. Immer, wenn die Datei vom Benutzer gespeichert wird, werden weitere Ereignisse produziert.

Wie Sie sehen können, kann die Auswertung der durch die Überwachung generierten Daten ohne geeignete Werkzeuge, wie zum Beispiel dem Microsoft Operations Manager, eine mühsame Aufgabe sein.

4

Zuweisen von Benutzerrechten

Benutzerrechte sind Aktionen, die ein Benutzer auf einem System oder in einer Domäne durchführen darf. Es gibt zwei Arten von Benutzerrechten: Anmelderechte und Privilegien. Anmelderechte legen fest, wer sich wie an einem Computer anmelden darf. Privilegien legen den Zugriff auf systemweite Ressourcen fest. Sie haben Vorrang vor den Zugriffsrechten von Objekten. Ein Beispiel für ein Anmelderecht ist das Recht, sich lokal an einem Computer anzumelden. Ein Beispiel für ein Privileg wäre das Recht, ein System herunterzufahren. Diese beiden Arten von Benutzerrechten werden für einzelne Benutzer und Gruppen vom Administrator über die Sicherheitseinstellungen vergeben. Eine Zusammenfassung der Standardwerte der Benutzerrechte, die in diesem Kapitel besprochen werden, finden Sie in der mitgelieferten Excel-Tabelle. Die Einstellungen für die Benutzerrechte können im Gruppenrichtlinieneditor über den folgenden Pfad vorgenommen werden: *Computerkonfiguration\Windows Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechten*

Die möglichen Werte für alle in diesem Kapitel besprochenen Einstellungen sind:

- **Eine benutzerdefinierte Liste von Konten**
- **Nicht konfiguriert**

Auf diesen Computer vom Netzwerk aus zugreifen

Dieses Recht erlaubt es einem Benutzer, sich über das Netzwerk mit dem Computer zu verbinden. Es ist für mehrere Netzwerkprotokolle, unter anderen SMB (Server Message Block), NetBIOS (Network Basic Input/Output System), CFIS (Common Internet File System) und COM+ (Component Object Model Plus) erforderlich.

Sicherheitslücken

Benutzer, die vom Netzwerk auf einen Computer zugreifen können, haben auch auf die Ressourcen dieses Computers Zugriff. Dieses Recht ist zum Beispiel notwendig, damit Benutzer auf freigegebene Drucker und Ordner zugreifen können. Wenn es der Gruppe **Jeder** zugewiesen ist, und diese Gruppe in den NTFS-Berechtigungen mindestens das Recht *Lesen* besitzt, dann ist jeder in der Lage, die entsprechenden Dateien anzuzeigen. Bei einer neuen Installation von Windows Server 2003 ist dies jedoch unwahrscheinlich, da in den Standardberechtigungen für Freigaben und NTFS unter Windows Server 2003 die Gruppe **Jeder** nicht enthalten ist. Bei Systemen, die von Windows NT 4.0 oder Windows 2000 aktualisiert wurden, könnte dies jedoch der Fall sein, da diese Betriebssysteme nicht so restriktiv arbeiten wie Windows Server 2003.

Gegenmaßnahmen

Schränken Sie das Recht auf die Benutzer ein, für die ein Zugriff auf den Server erforderlich ist. Wenn es zum Beispiel für die Gruppen **Administratoren** und **Benutzer** konfiguriert ist, sind alle an der Domäne angemeldeten Benutzer in der Lage auf die Server der Domäne zuzugreifen.

Mögliche Auswirkungen

Wenn das Recht den Benutzern auf den Domänencontrollern genommen wird, ist kein Benutzer mehr in der Lage, sich an den Domänen anzumelden oder Netzwerkressourcen zu verwenden. Wenn das

Recht auf Mitgliedsservern entfernt wird, können die Benutzer auf diese Server nicht mehr zugreifen. Aus diesen Gründen sollten Sie sichergehen, dass die autorisierten Benutzer das Recht für alle Computer des Netzwerkes auf die sie zugreifen müssen besitzen.

Einsetzen als Teil des Betriebssystems

Dieses Recht gestattet es einem Prozess, die Identität eines Benutzers zu verwenden. So bekommt er Zugriff auf die Ressourcen, auf die der Benutzer zugreifen kann. Normalerweise benötigen dieses Privileg nur Low Level Autorisierungsdienste. Beachten Sie, dass der potentielle Zugriff nicht auf die Objekte beschränkt ist, auf die der Benutzer Zugriff hat. Der Prozess kann eigenmächtig weitere Privilegien anfordern. Er könnte außerdem ein Zugriffs-Token erstellen, das im Überwachungsprotokoll ohne Identifizierung erscheint.

Sicherheitslücken

Dieses Benutzerrecht ist sehr mächtig. Jeder mit diesem Recht kann die komplette Kontrolle über den Computer übernehmen und möglicher Beweise für die eigenen Aktivitäten löschen.

Gegenmaßnahmen

Beschränken Sie das Recht auf so wenige Konten wie möglich. Es sollte unter normalen Umständen nicht einmal der Gruppe **Administratoren** zugewiesen werden. Wenn ein Dienst dieses Privileg erfordert, konfigurieren Sie den Dienst so, dass er ein lokales Systemkonto mit eingeschränkten Rechten verwendet. Erstellen Sie kein neues Konto, um diesem dann das Privileg zuzuweisen.

Mögliche Auswirkungen

Keine oder fast keine. Dieses Recht wird, außer vom lokalen Systemkonto, nur sehr selten benötigt.

Hinzufügen von Arbeitsstationen zur Domäne

Dieses Benutzerrecht gestattet es einem Benutzer, einen Computer zu einer Domäne hinzuzufügen. Damit das Privileg tatsächlich gültig ist, muss es über die *Default Domain Controllers Policy* einer Domäne zugewiesen werden. Ein Benutzer mit diesem Privileg kann bis zu zehn Arbeitsstationen zur Domäne hinzufügen. Wenn einem Benutzer das Recht Computerkonten zu erstellen für die Organisationseinheit (OU), in der sich die Computerkonten befinden, zugewiesen wurde, kann dieser auch ohne das Privileg unbegrenzt viele Arbeitsstationen in die Domäne aufnehmen.

Sicherheitslücken

Die Gefahr durch dieses Benutzerrecht ist ehr gering. Benutzer könnten mit ihm einen Computer zur Domäne hinzufügen und die Sicherheitsrichtlinien des Unternehmens unterlaufen. Wenn die Benutzer in Ihrer Organisation keine administrativen Rechte besitzen, können diese zum Beispiel Windows neu installieren und sich dann selbst administrative Rechte geben.

Gegenmaßnahmen

Vergeben Sie das Recht nur an autorisierte Mitglieder des IT-Teams.

Mögliche Auswirkungen

Wenn es den Benutzer vorher nicht gestattet war, ihre eigenen Computer zu installieren und in die Domäne aufzunehmen, gibt es keine Auswirkungen. Wenn dies jedoch vorher der Fall war, müssen hierfür neue Verfahren und Prozesse definiert werden.

Anpassen von Speicherkontingenten für einen Prozess

Dieses Benutzerrecht erlaubt es einem Benutzer den maximal für einen Prozess zur Verfügung stehenden Arbeitsspeicher festzulegen. Das Privileg ist zur Verbesserung der Systemleistung sehr brauchbar, kann jedoch in den falschen Händen auch missbraucht werden. Es könnte zum Beispiel für einen DoS-Angriff verwendet werden.

Sicherheitslücken

Ein Benutzer kann mit diesem Recht die für Prozesse zur Verfügung stehende Speichermenge reduzieren. So könnte er geschäftskritische Netzwerkanwendungen abstürzen lassen oder verlangsamen.

Gegenmaßnahmen

Beschränken Sie das Recht auf Benutzer, die es für die Durchführung ihrer Aufgaben benötigen. Zum Beispiel Anwendungsadministratoren, die für die Pflege von Datenbankmanagementsystemen verantwortlich sind.

Mögliche Auswirkungen

Organisationen, die bei der Einschränkung von Rechten und Privilegien für Benutzerrollen nachlässig waren, finden diese Maßnahmen möglicherweise schwer umzusetzen. Für die meisten Organisationen sollte diese Einschränkung jedoch keine Auswirkungen haben.

Lokal anmelden

Dieses Benutzerrecht gestattet dem Benutzer die Durchführung einer interaktiven Anmeldung am Computer. Benutzer, die dieses Recht nicht haben, sind weiterhin in der Lage sich über das Netzwerk am Computer anzumelden. Sie benötigen hierfür allerdings das Recht **Anmeldung über Terminaldienste zulassen**.

Sicherheitslücken

Wenn dieses Recht nicht auf die autorisierten Benutzer, die sich an einem Computer anmelden müssen, beschränkt wird, kann ein möglicher Angreifer mit physikalischem Zugriff auf den Computer eine Anmeldung durchführen. Er könnte dann zum Beispiel einen bösartigen Code ausführen, um seine Privilegien zu erweitern.

Gegenmaßnahmen

Auf Domänencontrollern sollte dieses Recht nur die Gruppe **Administratoren** besitzen. Für andere Serverrollen fügen Sie die Gruppen **Sicherungsoperatoren** und **Hauptbenutzer** hinzu. Auf Arbeitsstationen geben Sie zusätzlich der Gruppe **Benutzer** das Recht. Alternativ können Sie solche Gruppen wie **Kontooperatoren**, **Serveroperatoren** und **Gäste** mit in das Recht **Lokale Anmeldung verweigern** aufnehmen.

Mögliche Auswirkungen

Nur Benutzer mit den entsprechenden administrativen Rollen können eine lokale Anmeldung durchführen. Stellen Sie sicher, dass nicht versehentlich delegierte Aufgaben betroffen sind.

Anmeldung über Terminaldienste zulassen

Dieses Recht erlaubt es dem Benutzer, sich über eine Remotedesktopverbindung anzumelden. Sie sollten keinen weiteren Benutzer oder Gruppen zuweisen. Stattdessen fügen Sie die entsprechenden Benutzer der Gruppe **Remotedesktopbenutzer** hinzu.

Sicherheitslücken

Jedes Konto mit diesem Recht kann verwendet werden, um sich über das Netzwerk am Computer anzumelden. Ein Angreifer könnte eins dieser Konten missbrauchen, um zum Beispiel einen bösartigen Code auszuführen und seine Privilegien zu erweitern.

Gegenmaßnahmen

Auf Domänencontrollern geben Sie dieses Recht nur der Gruppe **Administratoren**. Bei anderen Serverrollen und auf Arbeitsstationen, fügen Sie die entsprechenden Benutzer zur Gruppe **Remotedesktopbenutzer** hinzu. Bei allen Serverrollen außer Terminalservern, die im Anwendungsmodus ausgeführt werden, stellen Sie sicher, dass zu dieser Gruppe nur die Mitglieder des IT-Teams gehören.

Warnung: Stellen Sie auf Terminalservern, die im Anwendungsmodus ausgeführt werden, sicher, dass nur die Benutzer der Gruppe **Remotedesktopbenutzer** angehören, die dieses Recht auch benötigen.

Alternativ können Sie Gruppen wie **Kontooperatoren**, **Serveroperatoren** und **Gäste** mit in das Privileg **Anmeldung über Terminaldienste verweigern** aufnehmen. Stellen Sie hierbei aber sicher, dass Sie nicht versehendlich einem legitimen Administrator dieses Recht verweigern.

Mögliche Auswirkungen

Nur die Benutzer mit den entsprechenden administrativen Rollen können sich noch über den Terminaldienst anmelden. Stellen Sie aber sicher, dass nicht versehendlich delegierte Aufgaben betroffen sind.

Sichern von Dateien und Verzeichnissen

Dieses Benutzerrecht gestattet es einem Benutzer zur Systemsicherung die Datei- und Ordnerberechtigungen zu umgehen. Es wird nur verwendet, wenn eine Anwendung einen Zugriff über die NTFS-Sicherungs API (Application Programming Interface) versucht.

Sicherheitslücken

Benutzer, die in der Lage sind Daten von einem Computer zu sichern, könnten diese auf ein Medium speichern, dass nicht der Domäne angehört und auf dem Sie administrative Rechte haben. Sie könnten dann den Besitz übernehmen und die gesicherten Daten anzeigen.

Gegenmaßnahmen

Beschränken Sie das Recht auf die Mitglieder des IT-Teams, die Sicherungen durchführen müssen.

Mögliche Auswirkungen

Das Ändern von Gruppenmitgliedschaften kann zu Einschränkungen der administrativen Fähigkeiten führen. Stellen Sie sicher, dass die Sicherungsadministratoren noch in der Lage sind, Sicherungen durchzuführen.

Auslassen der durchsuchenden Überprüfung

Ermöglicht dem Benutzer während der Navigation in einem Objektpfad eines Microsoft Windows-Dateisystems oder der Registrierung die Navigation in Ordnern, auf die der Benutzer normalerweise nicht zugreifen kann. Dieses Recht gestattet es dem Benutzer nicht, den Inhalt eines Ordners aufzulisten, sondern nur die zugehörigen Verzeichnisse zu „durchlaufen“.

Sicherheitslücken

Die Standardeinstellung dieses Privilegs gestattet das „Durchlaufen“ jedem Benutzer. Für erfahrene Windows-Administratoren entspricht dies ihren Erwartungen, und sie konfigurieren die Zugriffskontrolllisten (ACLs) des Dateisystems entsprechend. Das einzige Szenario, in dem die Standardeinstellung zu Problemen führen könnte, kommt zustande, wenn Administratoren die ACLs konfigurieren, ohne dieses Verhalten zu verstehen. Diese erwarten dann nämlich, dass die Benutzer bei einer Zugriffsverweigerung auf einen Ordner auch nicht in der Lage sind, auf dessen Unterordner zuzugreifen. Da dies jedoch sehr unwahrscheinlich ist, ist das Risiko dieses Privilegs sehr gering.

Gegenmaßnahmen

In Organisationen, in denen die Sicherheit einen extrem hohen Stellenwert hat, sollte die Gruppe **Jeder** oder vielleicht sogar die Gruppe **Benutzer** aus diesem Privileg entfernt werden.

Mögliche Auswirkungen

Das Betriebssystem und viele Anwendungen wurden in der Erwartung entwickelt, dass jeder Benutzer dieses Privileg besitzt. Daher kann das Entfernen der Gruppe **Jeder** aus diesem Recht zu einer Instabilität des Betriebssystems oder zu Anwendungsfehlern führen. Es wird empfohlen, die Einstellung auf ihrem Standardwert zu belassen.

Ändern der Systemzeit

Ermöglicht es dem Benutzer die Uhrzeit der internen Systemuhr einzustellen. Dieses Privileg ist für eine Änderung der Zeitzone oder der Anzeige der Systemzeit nicht notwendig.

Sicherheitslücken

Benutzer, die in der Lage sind die Uhrzeit auf einem Computer zu verstellen, könnten diverse Probleme verursachen: Zeitstempel in Einträgen im Ereignisprotokoll stimmen nicht mehr, Zeitstempel für das Erstellungs- oder Änderungsdatum von Dateien und Ordner sind falsch, und Computer, die einer Domäne angehören, könnten nicht mehr in der Lage sein, sich oder einen Benutzer, der sich anmelden will zu authentifizieren. Auf den meisten Domänencontrollern, Mitgliedsservern und Arbeitsstationen wird dieses Risiko dadurch minimiert, dass der **Windows Zeitgeber Dienst** die Uhrzeit automatisch mit dem Domänencontroller synchronisiert. Dies passiert folgendermaßen:

- Alle Clients und Mitgliedsserver erkennen den authentifizierenden Domänencontroller als ihren internen Synchronisationspartner.
- Alle Domänencontroller einer Domäne erkennen den PDC-Emulator (Primary Domain Controller) als internen Synchronisationspartner.
- Alle PDC-Emulatoren folgen bei der Erkennung ihrer internen Synchronisationspartner der Domänenhierarchie.
- Der PDC-Emulator der Stammdomäne ist die maßgebliche Zeitquelle der Organisation. Daher wird empfohlen, dass Sie ihn für die Synchronisation mit einer zuverlässigen externen Zeitquelle konfigurieren.

Ein Sicherheitsproblem entsteht, wenn ein Angreifer in der Lage ist, die Systemzeit zu ändern und dann den **Windows Zeitgeber Dienst** zu beenden. So würde keine Synchronisierung mehr durchgeführt werden.

Gegenmaßnahmen

Beschränken Sie dies Recht auf Benutzer, die es tatsächlich benötigen, wie zum Beispiel die Mitglieder des IT-Teams.

Mögliche Auswirkungen

Da in den meisten Organisationen die Zeitsynchronisation für die Computer der Domäne vollautomatisch durchgeführt wird, sollte es keine Auswirkungen geben. Computer die keiner Domäne angehören, sollten mit einer externen Quelle synchronisiert werden.

Erstellen einer Auslagerungsdatei

Dies Privileg gestattet es Benutzern die Größe der Auslagerungsdatei zu ändern.

Sicherheitslücken

Benutzer könnten die Auslagerungsdatei extrem verkleinern oder sie auf eine sehr ausgelastete Partition verschieben. Dies könnte zu einer Verschlechterung der Systemleistung führen.

Gegenmaßnahmen

Beschränken Sie das Privileg auf die Mitglieder der Gruppe **Administratoren**.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Erstellen eines Token-Objekts

Dieses Recht erlaubt es einem Prozess ein Token zu erstellen. Das Token kann dieser dann verwenden, um auf lokale Ressourcen zuzugreifen.

Sicherheitslücken

Das Betriebssystem legt den Zugriff des Benutzers fest, indem es das Zugriffstoken des Benutzers überprüft. Zugriffstoken werden erstellt, wenn ein Benutzer sich lokal anmeldet, oder wenn er sich über das Netzwerk mit einem anderen Computer verbindet. Wenn Sie dem Benutzer ein Recht nehmen, wird diese Änderung in der Registrierung sofort umgesetzt. Im Zugriffstoken des Benutzers wird sie jedoch erst bei seiner nächsten Anmeldung geändert.

Ein Benutzer, der in der Lage ist Tokens zu erstellen oder zu ändern, kann die Zugriffsrechte für jedes angemeldete Konto verändern. Er könnte zum Beispiel seine eigenen Privilegien erweitern oder das System in einen DoS-Zustand bringen.

Gegenmaßnahmen

Weisen Sie dies Recht keinem Benutzer zu. Prozesse, die dieses Recht unbedingt benötigen, sollten das lokale Systemkonto verwenden. Dies besitzt das Recht bereits.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Globale Objekte erstellen

Dies Recht ist notwendig, damit ein Benutzer Objekte erstellen kann, die in allen Sitzungen zur Verfügung stehen. Objekte für seine eigene Sitzung kann er auch ohne das Recht erstellen.

Sicherheitslücken

Benutzer, die globale Objekte erstellen können, könnten auf Prozesse Einfluss nehmen, die unter anderen Benutzersitzungen ausgeführt werden. Das könnte zu einer Vielzahl von Problemen, wie zum Beispiel Anwendungsfehlern oder beschädigten Daten, führen.

Gegenmaßnahmen

Beschränken Sie das Recht auf die Mitglieder der lokalen Gruppe **Administratoren**.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Erstellen von dauerhaft freigegebenen Objekten

Dies Recht erlaubt es Benutzern über die Objektverwaltung ein Verzeichnisobjekt zu erstellen. Das bedeutet, dass der Benutzer freigegebene Ordner, Drucker und andere Objekte erstellen kann. Das Privileg ist für Kernelmode-Komponenten, die den Objekt-Namensraum erweitern, gedacht. Diese besitzen es normalerweise schon. Daher ist es nicht notwendig, das Privileg manuell zuzuweisen.

Sicherheitslücken

Benutzer mit diesem Privileg könnten durch das Erstellen neuer freigegebener Objekte sensible Daten im Netzwerk veröffentlichen.

Gegenmaßnahmen

Weisen Sie das Privileg keinen Benutzer zu. Prozesse, die es zwingend benötigen, sollten das lokale Systemkonto verwenden. Dieses besitzt das Privileg bereits. Benutzer, die der lokalen Gruppe **Administratoren** angehören, werden auch weiterhin zum Erstellen, Ändern und Löschen von freigegebenen Ordnern und Druckern in der Lage sein.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Debuggen von Programmen

Dies Recht gestattet es Benutzern einen Debugger an einen Prozess anzuhängen. Es ermöglicht den Zugriff auf sensible und kritische Betriebssystemkomponenten.

Sicherheitslücken

Das Recht kann zum Erlangen von sensiblen Systeminformationen aus dem Speicher genutzt werden. Einige Werkzeuge können das Recht ausnutzen, um gehashte Passwörter oder andere private Sicherheitsinformationen zu extrahieren.

Gegenmaßnahmen

Entfernen Sie das Recht für alle Benutzer und Gruppen

Mögliche Auswirkungen

Die Entfernung dieses Rechtes wird dazu führen, dass niemand mehr in der Lage ist Programme zu debuggen. Unter normalen Umständen ist das Debuggen von Programmen auf Produktivsystemen allerdings selten notwendig. Wenn ein Problem auf einem Produktionsserver auftritt, dass ein zeitweises Debuggen von Programmen nötig macht, verschieben Sie den Server in eine andere OU und weisen Sie dem entsprechenden Konto das Recht zu.

Zugriff vom Netzwerk auf diesen Computer verweigern

Dieses Recht verbietet es Benutzern vom Netzwerk aus auf den Computer zuzugreifen.

Sicherheitslücken

Benutzer, die sich über das Netzwerk am Computer anmelden können, könnten sich die Kontennamen, die Gruppennamen und die freigegebenen Ressourcen auflisten lassen. Benutzer mit der Berechtigung auf freigegebene Ordner zuzugreifen, können möglicherweise Daten anzeigen oder verändern. Sie sollten Sich hiervor schützen, indem Sie Risikokonten, wie zum Beispiel dem lokalen Gastkonto oder anderen Konten, die keine Notwendigkeit haben über das Netzwerk auf den Computer zuzugreifen, das Recht explizit verweigern.

Gegenmaßnahmen

Verweigern Sie das Recht den folgenden Konten:

- Dem Konto ANONYMOUS LOGON.

- Dem lokalen Standardkonto Administrator.
- Dem lokalen Gastkonto.
- Das Standard-Supportkonto (das Konto Support_ 388945a0 wird für die Remoteunterstützung verwendet).
- Allen Dienstkonten.

Eine wichtige Ausnahme dieser Liste bilden alle Dienstkonten, die zum Starten von den Diensten verwendet werden, die notwendig sind den Computer über das Netzwerk zu verbinden. Wenn Sie zum Beispiel einen freigegebenen Ordner für einen Webserver konfiguriert haben, müssen Sie dem Konto, unter dem der Microsoft Internet Information Server (IIS) ausgeführt wird, den Zugriff gestatten.

Mögliche Auswirkungen

Die Möglichkeiten der administrativen Benutzer könnten eingeschränkt werden. Stellen Sie sicher, dass nicht versehendlich delegierte Aufgaben betroffen sind.

Anmeldung als Batchauftrag verweigern

Dieses Recht verhindert, dass ein Benutzer sich über die Verwendung eines Batchauftrags anmeldet. Mit Batchauftrag ist das Feature des Windows Server 2003 gemeint, dass für die Zeitplanung von Tasks über den Taskplaner verwendet wird. Das Recht wird von allen Konten benötigt, die für die Planung von automatischen Tasks über den Taskplaner verwendet werden.

Sicherheitslücken

Konten mit diesem Recht könnten Tasks planen, die sehr viele Systemressourcen belegen. Dies könnte zu einem DoS-Zustand führen.

Gegenmaßnahmen

Weisen Sie das Recht den Standardkonten **Support**, Support_ 388945a0 und dem lokalen Gastkonto zu.

Mögliche Auswirkungen

Wenn das Recht anderen Konten zugewiesen wird, könnte es Benutzer mit speziellen administrativen Aufgaben unmöglich werden diese auszuführen. Stellen Sie sicher, dass nicht versehendlich delegierte Aufgaben betroffen sind.

Anmeldung als Dienst verweigern

Dieses Recht verbietet es Benutzern sich als Dienst anzumelden.

Sicherheitslücken

Konten, die sich als Dienst anmelden können, könnten zum Starten neuer, nicht autorisierter Dienste, wie zum Beispiel einem Trojanischen Pferd oder einer Hintertür, verwendet werden. Eine Hintertür ist ein versteckter Zugang zum Betriebssystem, über den Systeminformationen abgerufen werden können. Gegenmaßnahmen hierzu sind nur bedingt nützlich, da ein Angreifer, der bereits Zugriffsrechte erlangt hat, einen Dienst auch unter dem lokalen Systemkonto ausführen kann.

Gegenmaßnahmen

Weisen Sie das Recht keinem Konto zu. Organisationen, in denen die Sicherheit einen sehr hohen Stellenwert hat, können das Recht allen Gruppen, die niemals von einem Dienst verwendet werden, zuweisen.

Mögliche Auswirkungen

Wenn Sie das Recht bestimmten Konten zuweisen, könnte es sein, dass Dienste nicht mehr gestartet werden. Dies könnte zu einem DoS-Zustand führen.

Lokale Anmeldung verweigern

Dies Recht verbietet den Benutzern sich direkt über die Tastatur des Computers anzumelden.

Sicherheitslücken

Jedes Konto, das in der Lage ist, sich direkt am Computer anzumelden, könnte von einem Angreifer zur Ausführung von schädlichem Programmcode oder zur Erweiterung der eigenen Privilegien verwendet werden.

Gegenmaßnahmen

Weisen Sie dem Standardkonto **Support** dieses Recht zu.

> **Anmerkung:** Das Konto Support_388945a0 stellt die Hilfe- und Supportdienste über signierte Scripts zur Verfügung. Administratoren können über dieses Konto die Fähigkeit zum ausführen von signierten Scripten an normale Benutzer delegieren. Das Konto hat nur beschränken Zugriff auf den Computer und ist standardmäßig deaktiviert.

Mögliche Auswirkungen

Wenn Sie das Recht weiteren Konten zuweisen, könnte es sein, dass Benutzer mit administrativen Aufgaben nicht mehr in der Lage sind diese auszuführen. Stellen Sie sicher, dass nicht versehentlich delegierte Aufgaben betroffen sind.

Anmeldung über Terminaldienste verweigern

Dies Recht verweigert den Benutzern die Anmeldung an einen Computer über eine Remotedesktopverbindung.

Sicherheitslücken

Jedes Konto, das in der Lage ist sich über den Terminaldienst am Computer anzumelden, könnte von einem Angreifer zur Ausführung von schädlichem Programmcode oder zur Erweiterung der eigenen Privilegien verwendet werden.

Gegenmaßnahmen

Weisen Sie das Recht dem lokalen Standardkonto **Administrator** und allen **Dienstkonten** zu.

Mögliche Auswirkungen

Wenn Sie das Recht weiteren Konten zuweisen, könnte es sein, dass Benutzer mit administrativen Aufgaben nicht mehr in der Lage sind diese auszuführen. Stellen Sie sicher, dass nicht versehentlich delegierte Aufgaben betroffen sind.

Ermöglichen, dass Computer- und Benutzerkonten für Delegierungszwecke vertraut wird

Dieses Privileg gestattet es Benutzern die Einstellung **Für Delegierungszwecke vertrauen** eines Objektes in Active Directory zu ändern. Der Benutzer oder Computer dem es zugewiesen wird, muss zusätzlich Schreibzugriff auf die entsprechenden Attribute des Objekts haben.

Multi-tier Client/Server Anwendungen sind in der Lage die Authentifizierung zu delegieren. Dies gestattet es einem Frontend-Dienst die Anmeldeinformationen eines Clients für die Authentifizierung bei einem Backend-Dienst zu verwenden. Damit dies möglich ist, müssen sowohl Client als auch Server unter einem Konto ausgeführt werden, dem für Delegierungszwecke vertraut wird.

Sicherheitslücken

Ein Missbrauch dieses Privilegs könnte dazu führen, dass sich unautorisierte Benutzer als legale Benutzer ausgeben. Ein Angreifer könnte es ausnutzen, um Zugriff auf Netzwerkressourcen zu erlangen. Solche Angriffe sind häufig sehr schwer zu verfolgen.

Gegenmaßnahmen

Weisen Sie dieses Privileg nur der Gruppe **Administratoren** auf den **Domänencontrollern** zu.

> **Anmerkung:** Es gibt auf Mitgliedsservern und Arbeitsstationen einer Domäne keinen Grund das Privileg irgendjemandem zuzuweisen. In diesen Kontexten hat es keine Bedeutung. Es ist nur auf Domänencontrollern oder eigenständigen Systemen von Relevanz.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Erzwingen des Herunterfahrens von einem Remotesystem aus

Dies Privileg erlaubt es Benutzern einen Computer über das Netzwerk herunterzufahren.

Sicherheitslücken

Jeder Benutzer, der einen Computer herunterfahren kann, kann einen DoS-Zustand herbeiführen. Daher sollte dies Privileg sehr restriktiv vergeben werden.

Gegenmaßnahmen

Beschränken Sie das Privileg auf die Mitglieder der Gruppe **Administratoren**.

Mögliche Auswirkungen

Wenn Sie die Gruppe **Serveroperatoren** aus diesem Recht entfernen, könnte es sein, dass Benutzer mit administrativen Aufgaben nicht mehr in der Lage sind diese auszuführen. Stellen Sie sicher, dass nicht versehendlich delegierte Aufgaben betroffen sind.

Generieren von Sicherheitsüberwachungen

Dies Recht erlaubt es einem Prozess Überwachungseinträge im Sicherheitsprotokoll zu erzeugen. Das Sicherheitsprotokoll kann zu Erkennung von nicht autorisierten Systemzugriffen verwendet werden.

Sicherheitslücken

Konten, die in der Lage sind in das Sicherheitsprotokoll zu schreiben, könnten von einem Angreifer dazu verwendet werden, das Protokoll mit sinnlosen Einträgen zu füllen. Wenn der Computer so konfiguriert ist, dass Ereignisse bei Bedarf überschrieben werden, kann der Angreifer über diesen Weg die Beweise für seine Aktivitäten beseitigen. Wenn der Computer so konfiguriert ist, dass er heruntergefahren wird wenn das Protokoll voll ist, kann der Angreifer so einen DoS-Zustand herbeiführen.

Gegenmaßnahmen

Stellen Sie sicher, dass nur die Gruppen **Lokale Dienste** und **Netzwerkdienst** über dieses Privileg verfügen.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Annehmen der Clientidentität nach Authentifizierung

Wenn dieses Privileg einem Benutzer zugewiesen wird, dann können Programme unter der Identität des Benutzers ausgeführt werden. Den Diensten, die vom Service Control Manager gestartet werden, wird zum Zugriffstoken standardmäßig die Gruppe Dienste hinzugefügt. Dies gilt auch für COM-Server, die durch die COM-Infrastruktur gestartet werden. Das führt dazu, dass solche Dienste über dieses Recht verfügen. Außerdem kann ein Benutzer eine Clientidentität annehmen, wenn eine der folgenden Bedingungen zutrifft:

- Das Zugriffstoken ist für den Benutzer vorgesehen.
- Der meldet sich mit expliziten Anmeldeinformationen an.
- Der angeforderte Zugriff ist geringer als der der Clientidentität. (zum Beispiel anonym)

Aufgrund dieser Faktoren benötigt der Benutzer dieses Recht normalerweise nicht.

Sicherheitslücken

Ein Benutzer mit diesem Privileg könnte einen Client so überlisten, dass er eine Verbindung mit einem Dienst aufbaut, den der Benutzer eingerichtet hat. Dann könnte er die Clientidentität annehmen und seine eigenen Rechte erweitern.

Gegenmaßnahmen

Stellen Sie sicher, dass nur die Gruppen **Administratoren** und **Dienste** dieses Privileg besitzen.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Anheben der Zeitplanungspriorität

Dies Privileg gestattet es Benutzern die Basispriorität von Prozessen anzuheben. Es ermöglicht nicht das Anheben der relativen Priorität. Es wird für die Verwendung der mit dem Betriebssystem zur Verfügung gestellten administrativen Werkzeuge nicht benötigt. Es könnte aber für die Verwendung von Werkzeugen zur Softwareentwicklung notwendig sein.

Sicherheitslücken

Ein Benutzer mit diesem Privileg könnte die Priorität eines Prozesses auf „Echtzeit“ heraufsetzen. Damit stünde anderen Prozessen nur noch minimale Rechenzeit zur Verfügung, und es würde ein DoS-Zustand entstehen.

Gegenmaßnahmen

Stellen Sie sicher, dass nur die Gruppe **Administratoren** über das Privileg verfügt.

Mögliche Auswirkungen

Keine, da dies die Standardkonfiguration ist.

Laden und Entfernen von Gerätetreibern

Dies Privileg legt fest, ob Benutzer Gerätetreiber dynamisch laden und entladen können. Das Recht ist nicht notwendig, wenn für ein neues Gerät bereits ein signierter Treiber in der Datei Driver.cab des Computers existiert.

Sicherheitslücken

Treiber werden mit sehr weitreichenden Privilegien ausgeführt. Ein Benutzer, der über das Privileg verfügt Treiber zu laden und zu entladen, könnte versehentlich als Treiber getarnten schädlichen Programmcode installieren. Es wird davon ausgegangen, dass Administratoren hier mehr Vorsicht walten lassen und nur digital signierte Treiber installieren.

> **Anmerkung:** Um für einen lokalen Drucker einen neuen Treiber zu installieren oder um diesen verwalten zu können, müssen Sie seit Windows XP bzw. Windows Server 2003 über das Recht verfügen und Mitglied der Gruppen Administratoren oder Hauptbenutzer sein.

Gegenmaßnahmen

Weisen Sie das Recht ausschließlich der Gruppe **Administratoren** zu.

Mögliche Auswirkungen

Wenn Sie der Gruppe **Druckoperatoren** dieses Recht nehmen, könnten diese bei der Durchführung ihrer Aufgaben eingeschränkt werden. Stellen Sie sicher, dass nicht versehendlich delegierte Aufgaben betroffen sind.

Sperren von Seiten im Speicher

Dieses Privileg erlaubt es Prozessen Daten im physikalischen Speicher zu halten. Das verhindert, dass das System diese Daten in den virtuellen Speicher auslagert. Wenn Sie dieses Privileg vergeben, kann das zu einer deutlichen Verschlechterung der Systemleistung führen.

Sicherheitslücken

Ein Benutzer mit diesem Privileg kann mehren Prozessen physikalischen Speicher zuweisen. Damit stände anderen Prozessen wenig oder kein Arbeitsspeicher mehr zur Verfügung. So könnte es zu einem DoS-Zustand kommen.

Gegenmaßnahmen

Vergeben Sie das Recht nicht.

Mögliche Auswirkungen

Keine, da dies die Standardkonfiguration ist.

Anmelden als Stapelverarbeitungsauftrag

Dieses Recht erlaubt es Benutzern sich über eine Stapelverarbeitung, wie zum Beispiel den Taskplanerdienst, anzumelden. Wenn ein Administrator einen Task zur Ausführung eines bestimmten Benutzerkontos plant, dann wird diesem Konto automatisch dieses Recht zugewiesen. Wenn der Task dann ausgeführt wird, meldet der Taskplanerdienst den Benutzer als Stapelverarbeitungsauftrag an. Der Task wird dann im Sicherheitskontext des Benutzers ausgeführt.

Sicherheitslücken

Die Risiken sind eher gering. Für die meisten Organisationen sind die Standardeinstellungen ausreichend.

Gegenmaßnahmen

Wenn Sie möchten, dass Tasks unter einem bestimmten Konto ausgeführt werden können, dann sollten Sie es dem System ermöglichen, das Recht automatisch zuzuweisen. Wenn Sie das nicht möchten, sollten Sie das Recht ausschließlich für die lokalen Dienstkonten und das Supportkonto (Support_388945a0) konfigurieren. Auf IIS-Servern sollten Sie diese Richtlinie lokal konfigurieren. So stellen Sie sicher, dass die lokalen Konten **IUSR_computername** und **IWAM_computername** über das Recht verfügen.

Mögliche Auswirkungen

Wenn Sie das Recht über domänenbasierte Gruppenrichtlinien zuweisen, ist das System nicht in der Lage, das Recht über den Taskplaner zuzuweisen, und den Konten IUSR_computername und IWAM_computername fehlt es ebenfalls. Die IIS sind somit nicht mehr in der Lage, die notwendigen COM-Komponenten auszuführen.

Als Dienst anmelden

Dies Recht erlaubt es einem Sicherheitsprinzipal sich als Dienst anzumelden. Dienste können zur Ausführung unter dem lokalen Konto **System**, dem Konto **lokaler Dienst** oder dem Konto **Netzwerkdienst** konfiguriert werden. Diese Konten besitzen das Recht bereits. Für jedes andere Konto, unter dem ein Dienst ausgeführt werden soll, muss das Recht zuwiesen werden.

Sicherheitslücken

Dieses Recht ist sehr mächtig. Es erlaubt es Konten Netzwerkdienste zu starten. Die Risiken werden dadurch verringert, dass es nur Konten mit administrativen Privilegien gestattet ist Dienste zu installieren und zu konfigurieren. Ein Angreifer, der einen solchen administrativen Zugriff bereits erlangt hat, könnte einen Dienst auch unter dem lokalen Konto **System** ausführen.

Gegenmaßnahmen

Der Standardsicherheitsprinzipal, der dieses Recht besitzt, ist die lokale Standardgruppe **Netzwerkdienst**. Dienstkonten sollten dieser Gruppe hinzugefügt werden. Sie sollten die Mitgliedschaften dieser Gruppe überwachen, um Änderungen zu bemerken.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Verwalten von Überwachungs- und Sicherheitsprotokollen

Dieses Recht erlaubt es Benutzern die Überwachungsoptionen für Ressourcen, wie zum Beispiel Dateien, Active Directory Objekte und Registrierungsschlüssel, zu bearbeiten. Die Zugriffsüberwachung wird erst durchgeführt, wenn Sie diese über die **Überwachungsrichtlinie** aktivieren. Ein Benutzer mit diesem Privileg kann außerdem über die Ereignisanzeige das Sicherheitsprotokoll anzeigen und löschen.

Sicherheitslücken

Das Privileg ist sehr mächtig, und es sollte nur sehr eingeschränkt vergeben werden. Jeder, der es besitzt, kann das Sicherheitsprotokoll löschen und Beweise für nicht autorisierte Aktivitäten entfernen.

Gegenmaßnahmen

Stellen Sie sicher, dass nur die lokale Gruppe **Administratoren** über dieses Privileg verfügt.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Verändern der Firmwareumgebungsvariablen

Das Recht ermöglicht die Veränderung der Umgebungsvariablen durch einen Prozess über eine API, oder durch einen Benutzer über die Systemeigenschaften.

Sicherheitslücken

Jeder mit diesem Privileg könnte die Einstellungen einer Hardwarekomponente so ändern, dass diese nicht mehr funktionstüchtig ist. Dies könnte zur Beschädigung von Daten oder einem DoS-Zustand führen.

Gegenmaßnahmen

Stellen Sie sicher, dass nur die lokale Gruppe **Administratoren** über dieses Privileg verfügt.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Durchführen von Volumenwartungsaufgaben

Dieses Recht erlaubt es einen nicht-administrativen Benutzer oder einem Remotebenutzer Volumes oder Partitionen zu verwalten. Wenn ein Prozess, der im Sicherheitskontext des Benutzers ausgeführt wird, die Funktion SetFileValidData() aufruft, prüft Windows Server 2003 das Zugriffstoken des Benutzers auf dieses Privileg.

Sicherheitslücken

Ein Benutzer mit diesem Privileg könnte eine Partition oder ein Volumen löschen und so einen Datenverlust oder einen DoS-Zustand provozieren.

Gegenmaßnahmen

Stellen Sie sicher, dass nur die lokale Gruppe **Administratoren** über dieses Privileg verfügt.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Erstellen eines Profils für einen Einzelprozess

Dieses Recht erlaubt es Benutzern die Leistung eines Anwendungsprozesses zu messen. Normalerweise benötigen Sie dieses Privileg zur Verwendung des Snap-Ins Leistungsüberwachung nicht. Es sei denn, Sie möchten eine Leistungsüberwachung über Windows Management Instrumentation (WMI) konfigurieren.

Sicherheitslücken

Die Sicherheitsrisiken sind gering. Ein Angreifer mit diesem Privileg könnte die Leistung eines Computers überwachen. So könnte er herausfinden, welche Prozesse ausgeführt werden und Sicherheitsmaßnahmen wie Systeme zu Angriffserkennung und Virenscanner erkennen.

Gegenmaßnahmen

Stellen Sie sicher, dass nur die lokale Gruppe **Administratoren** über dieses Privileg verfügt.

Mögliche Auswirkungen

Wenn Sie der Gruppe **Hauptbenutzer** oder anderen Konten dieses Recht nehmen, könnten diese bei der Durchführung ihrer administrativen Aufgaben eingeschränkt werden. Stellen Sie sicher, dass nicht versehendlich delegierte Aufgaben betroffen sind.

Erstellen eines Profils der Systemleistung

Dieses Recht erlaubt es Benutzern die Leistung eines Systemprozesses zu messen. Normalerweise benötigen Sie dieses Privileg zur Verwendung des Snap-Ins Leistungsüberwachung nicht. Es sei denn, Sie möchten eine Leistungsüberwachung über Windows Management Instrumentation (WMI) konfigurieren.

Sicherheitslücken

Die Sicherheitsrisiken sind gering. Ein Angreifer mit diesem Privileg könnte die Leistung eines Computers überwachen. So könnte er herausfinden, welche Prozesse ausgeführt werden und Sicherheitsmaßnahmen wie Systeme zu Angriffserkennung und Virenscanner erkennen.

Gegenmaßnahmen

Stellen Sie sicher, dass nur die lokale Gruppe **Administratoren** über dieses Privileg verfügt.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Entfernen des Computers von der Dockingstation

Dieses Recht gestattet es Benutzern einen tragbaren Computer über die Funktion **PC auswerfen** im **Startmenü** abzudocken.

Sicherheitslücken

Jeder mit diesem Recht kann einen gestarteten Computer aus einer Dockingstation entfernen. Der Wert dieser Einstellung wird jedoch durch mehrere Faktoren reduziert: Wenn ein Angreifer einen Computer neu starten kann, könnte er ihn nach dem Start des BIOS, aber vor dem Start des Betriebssystems, entfernen. Server sind von der Einstellung normalerweise nicht betroffen, da diese ehr selten in einer Dockingstation betrieben werden. Und letztendlich könnten Angreifer den Computer auch zusammen mit der gesamten Dockingstation stehlen.

Gegenmaßnahmen

Stellen Sie sicher, dass über dieses Recht nur die lokalen Gruppen **Administratoren** und **Hauptbenutzer** verfügen.

Mögliche Auswirkungen

Da es sich hierbei um die Standardkonfiguration handelt, sollten die Auswirkungen minimal sein. Wenn die Benutzer Ihrer Organisation keine Mitglieder der Gruppen **Administratoren** oder **Hauptbenutzer** sind, werden diese nicht mehr in der Lage sein, ihre eigenen tragbaren Computer

ohne ein Herunterfahren des Systems aus der Dockingstation zu entfernen. In diesem Fall sollten Sie der Gruppe **Benutzer** das Recht ebenfalls gewähren.

Ersetzen eines Tokens auf Prozessebene

Dieses Recht erlaubt es einem übergeordneten Prozess auf das Zugriffstoken eines untergeordneten Prozesses zuzugreifen.

Sicherheitslücken

Ein Benutzer, der über dieses Privileg und das Recht zur Anhebung der Speicherverwendung Prozessen verfügt, ist in der Lage Prozesse unter dem Sicherheitskontext eines anderen Benutzers zu starten. Nicht autorisierte Aktionen könnten so vor Beobachtern verborgen werden.

Gegenmaßnahmen

Stellen Sie sicher, dass nur die lokalen Gruppen **Lokaler Dienst** und **Netzwerkdienst** über dieses Recht verfügen.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Wiederherstellen von Dateien und Verzeichnissen

Dieses Recht ermöglicht es Benutzern, bei der Wiederherstellung Datei- und Ordnerberechtigungen zu umgehen und jeden gültigen Sicherheitsprinzipal als Besitzer zu konfigurieren.

Sicherheitslücken

Ein Angreifer mit diesem Privileg könnte sensible Unternehmensdaten auf einem System wiederherstellen. Hierbei könnte er aktuellere Daten überschreiben. Das könnte zu einem Verlust wichtiger Daten oder einem DoS-Zustand führen.

> **Anmerkung:** Die vorgeschlagenen Maßnahmen verhindern nicht, dass ein Angreifer Daten auf einem nicht verwalteten System wiederherstellt. Organisationen sollten daher die Medien, die sie zur Sicherung von Daten verwenden, gut schützen.

Gegenmaßnahmen

Stellen Sie sicher, dass nur die lokale Gruppe **Administratoren** über dieses Recht verfügt.

Mögliche Auswirkungen

Wenn der Gruppe **Sicherungsoperatoren** dieses Recht genommen wird, könnte es für Benutzer, denen bestimmte Aufgaben delegiert wurden, unmöglich werden diese durchzuführen. Stellen Sie sicher, dass die Änderungen sich nicht negativ auf die Arbeit der Benutzer auswirken.

Herunterfahren des Systems

Dieses Privileg erlaubt es Benutzern, den lokalen Computer herunterzufahren.

Sicherheitslücken

Auf Domänencontrollern sollte dieses Recht auf eine sehr kleine Gruppe von vertrauenswürdigen Administratoren beschränkt sein - auch wenn das Herunterfahren des Systems erst einmal die Möglichkeit erfordert, sich am System anmelden zu können. Das Herunterfahren eines Domänencontrollers führt natürlich dazu, dass dieser für Funktionen wie Anmeldungen, Verteilung von Gruppenrichtlinien und LDAP-Anfragen (Lightweight Directory Access Protocol) nicht mehr zu Verfügung steht. Die Auswirkungen auf die Domäne sind beim Herunterfahren von Domänencontroller die FSMO-Rollen (Flexible Single Master Operations) ausführen, wie zum Beispiel die Verarbeitung von Anmeldungen durch den PDC-Emulator (Primary Domain Controller), sind verheerend.

Gegenmaßnahmen

Stellen Sie sicher, dass auf Mitgliedsservern nur die Gruppen **Administratoren** und **Sicherungsoperatoren,** und auf Domänencontrollern nur die **Administratoren** in der Lage sind das System herunterzufahren.

Mögliche Auswirkungen

Wenn Sie diesen Standardgruppen dieses Recht nehmen, könnten diese bei der Durchführung ihrer administrativen Aufgaben eingeschränkt werden. Stellen Sie sicher, dass nicht versehendlich delegierte Aufgaben betroffen sind.

Synchronisieren von Verzeichnisdienstdaten

Dieses Recht ermöglicht es einem Prozess alle Objekte und Eigenschaften des Verzeichnisses zu lesen, und zwar unabhängig davon, wie diese geschützt sind. Es wird für die Verwendung des Dienstes LDAP-Verzeichnissynchronisation (Dirsync) benötigt.

Sicherheitslücken

Dieses Privileg wirkt sich auf Domänencontrollern aus. Nur sie sollten in der Lage sein die Daten des Verzeichnisses zu synchronisieren. Sie erhalten das Recht, wenn eine Synchronisation im Kontext des Systemkontos des Domänencontrollers durchgeführt wird. Ein Angreifer, der dieses Privileg besitzt, kann alle Informationen die im Verzeichnis gespeichert sind abrufen. Mit diesen Informationen, zum Beispiel Telefonnummern oder Adressen, könnte er weitere Angriffe durchführen, um so an sensible Unternehmensdaten zu gelangen,

Gegenmaßnahmen

Stellen Sie sicher, dass dieses Recht keinem Konto zugewiesen ist.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Übernehmen des Besitzes von Dateien und Objekten

Dieses Recht erlaubt es Benutzern den Besitz von abgesicherten Objekten zu übernehmen. Dies

betrifft Active Directory Objekte, NTFS-Dateien und -Ordner, Registrierungsschlüssel, Dienste und Prozesse.

Sicherheitslücken

Jeder Benutzer mit diesem Recht kann, unabhängig von den Berechtigungen des Objekts, die Kontrolle über ein Objekt erlangen. Er kann dann beliebige Aktionen mit diesem Objekt durchführen. Das könnte zu einem Datenverlust, einer Kompromittierung von Daten oder einem DoS-Zustand führen.

Gegenmaßnahmen

Stellen Sie sicher, dass dieses Recht ausschließlich der lokalen Gruppe **Administratoren** zugewiesen ist.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

5
Sicherheitsoptionen

Der Abschnitt *Sicherheitsoptionen* einer Gruppenrichtlinie aktiviert oder deaktiviert die Sicherheitseinstellungen eines Computers. Mögliche Einstellungen betreffen zum Beispiel die digitale Signierung, die Namen des Administrator- und Gastkontos, Zugriff auf Disketten und CD-ROMs, das Verhalten bei Installation von Treibern und Anmeldenachrichten. Die Standardeinstellungen finden Sie in der Excel-Tabelle *Windows Standardeinstellungen für Sicherheit und Dienste.xls*, die Sie mit diesem Handbuch zusammen erhalten haben. Sie können die Sicherheitsoptionen über den folgenden Pfad konfigurieren:
Computerkonfiguration\Windows Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen

Konten: Administratorkontostatus

Diese Einstellung aktiviert oder deaktiviert das Administratorkonto. Beim Start im abgesicherten Modus steht das Konto, unabhängig von dieser Einstellung, immer zur Verfügung.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Für manche Organisationen ist eine regelmäßige Änderung der Passwörter von lokalen Konten eine mühsame Aufgabe. Eine Alternative wäre die Deaktivierung des lokalen Administratorkontos. Ein weiterer Grund hierfür wäre, dass es nicht gesperrt wird, egal wie viele fehlgeschlagene Anmeldeversuche mit ihm durchgeführt werden. Das Konto wird so zum primären Ziel für Brute-Force-Angriffe. Außerdem ist sein Security Identifier (SID) allgemein bekannt und es gibt Werkzeuge von Drittanbietern, die eine Netzwerkauthentifizierung über eine SID statt einen Kontonamen ermöglichen. Das bedeutet für Sie, dass ein Angreifer auch nach der Umbenennung des Administratorkontos einen Brute-Force-Angriff über die SID durchführen könnte.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Deaktiviert**, so dass das Administratorkonto nicht mehr zu Verfügung steht.

Mögliche Auswirkungen

Das Deaktivieren des Kontos kann unter Umständen zu Problemen führen. Wenn aus irgendeinem Grund zum Beispiel in einer Domänenumgebung der Beitritt zur Domäne nicht funktioniert und es kein lokales Administratorkonto gibt, müssen Sie den Computer im abgesicherten Modus starten, um das Problem zu beheben. In dem Fall ist es vielleicht nicht möglich, das Konto wieder zu aktivieren. Es müsste dann ein anderes Mitglied der Gruppe Administratoren erst das Passwort des Administratorkontos ändern.

Konten: Gastkontenstatus

Diese Sicherheitseinstellung bestimmt, ob das Gastkonto aktiviert oder deaktiviert ist.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Indem sie sich als **Gast** anmelden, könnten nicht authentifizierte Netzwerkbenutzer über dieses Konto einen Systemzugriff erlangen und auf Ressourcen zugreifen. Und zwar auf alle Ressourcen, die den Zugriff für das Gastkonto, die Gruppe **Gäste** oder die Gruppe **Jeder** gestatten. So könnte es zum Verlust oder einer Kompromittierung von Daten kommen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Deaktiviert**, so dass das Gastkonto nicht mehr zu Verfügung steht.

Mögliche Auswirkungen

Alle Netzwerkbenutzer müssen sich vor einem Zugriff auf die freigegebenen Ressourcen des Systems authentifizieren. Wenn das Gastkonto deaktiviert ist, und die Option **Netzwerkzugriff: Freigabe- und Sicherheitsmodel** auf die Einstellung **Nur Gast** gesetzt ist, schlagen anonyme Netzwerkanmeldungen fehl. Solche Netzwerkanmeldungen werden zum Beispiel vom Microsoft Network Server (SMB-Dienst) durchgeführt. Da die Standardeinstellung unter Windows Server 2003, Windows 2000 und Windows XP **Deaktiviert** ist, sollten die Auswirkungen für die meisten Organisationen gering sein.

Konten: Lokale Kontenverwendung von leeren Kennwörtern auf Konsolenanmeldung beschränken

Diese Sicherheitseinstellung bestimmt, ob interaktive Remoteanmeldungen durch Netzwerkdienste, zum Beispiel Terminaldienste, Telnet und das File Transfer Protokoll (FTP) für lokale Konten ohne Passwort gestattet sind. Wenn diese Richtlinie aktiviert ist, können sich lokale Konten ohne Passwort nur über die Tastatur des Computers anmelden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Diese Einstellung betrifft nicht die Anmeldung direkt über die Tastatur des Computers oder Anmeldungen mit Domänenkonten.

Achtung: Anwendungen von Drittanbietern umgehen diese Einstellung möglicherweise.

Sicherheitslücken

Leere Passwörter sind für die Sicherheit eines Computers ein ernstes Problem. Daher sollten sie

durch die Sicherheitsrichtlinien des Unternehmens und durch technische Maßnahmen verhindert werden. Die Standardeinstellungen einer Windows Server 2003 Active Directory® Domäne erfordern daher auch komplexe Passwörter mit sieben oder mehr Zeichen. Trotzdem könnte ein Benutzer, der in der Lage ist neue Konten zu erstellen, für neue Konten die Passwortrichtlinien so umgehen, dass er leere Passwörter verwenden kann.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Keine, da es sich um die Standardeinstellung handelt.

Konten: Administrator umbenennen

Diese Einstellung legt den Kontonamen fest, der für die SID des Administratorkontos verwendet wird.

Die möglichen Werte für diese Einstellung sind:

- **Ein benutzerdefinierter Text**
- **Nicht konfiguriert**

Sicherheitslücken

Das Administratorkonto existiert auf allen Windows 2000-, Windows Server 2003- und Windows XP Professional-Computern. Daher sollte es Angreifern durch eine Umbenennung schwerer gemacht werden, durch einfaches Raten einen Zugriff über dieses privilegierte Konto zu erlangen. Das Administratorkonto kann normalerweise nicht gesperrt werden. Dabei ist es egal, wie oft ein Angreifer einen fehlgeschlagenen Anmeldeversuch durchführt. Aus diesem Grund ist das Administratorkonto natürlich ein häufiges Ziel für Brute-Force-Angriffe.

Das Umbenennen des Kontos hat allerdings nur einen eingeschränkten Wert, da das Konto auf jedem System die gleiche, allgemein bekannte SID verwendet. Es existieren Werkzeuge, über die Brute-Force-Angriffe durch die Verwendung der SID ermöglicht werden. In diesem Fall ist es egal, ob Sie das Konto umbenannt haben oder nicht.

Gegenmaßnahmen

Geben Sie über die Einstellung einen neuen Namen für das Administratorkonto an.

Mögliche Auswirkungen

Sie müssen die entsprechenden Benutzer über den neuen Namen des Kontos informieren.

Konten: Gastkonto umbenennen

Diese Einstellung legt den Kontonamen fest, der für die SID des Gastkontos verwendet wird.

Die möglichen Werte für diese Einstellung sind:

- **Ein benutzerdefinierter Text**

- **Nicht konfiguriert**

Sicherheitslücken

Das Administratorkonto existiert auf allen Windows 2000-, Windows Server 2003- und Windows XP Professional-Computern. Daher sollte es Angreifern durch eine Umbenennung schwerer gemacht werden, durch einfaches Raten einen Zugriff über dieses Konto zu erlangen.

Gegenmaßnahmen

Geben Sie über die Einstellung einen neuen Namen für das Gastkonto an.

Mögliche Auswirkungen

Da das Gastkonto unter Windows Server 2003, Windows 2000 und Windows XP als Standardeinstellung deaktiviert ist, sollte es keine Auswirkungen geben.

Überwachung: Zugriff auf globale Systemobjekte prüfen

Wenn diese Einstellung aktiviert ist, werden Systemobjekte, wie zum Beispiel DOS-Geräte, mit einer Standard-SACL (System Access Control List) erstellt. Wenn die Einstellung **Überwachung: Objektzugriff überwachen** ebenfalls aktiviert ist, werden die Zugriffe auf solche Systemobjekte außerdem überwacht.

Globale Systemobjekte, auch Basis-Systemobjekte oder Base Named Objects genannt, sind kurzlebige Kernelobjekte, denen ihre Namen von der Anwendung oder der Systemkomponente zugewiesen werden, die sie erstellt hat. Sie werden normalerweise verwendet, um Anwendungen zu synchronisieren. Da sie einen Namen haben, sind diese Objekte für alle Prozesse des Systems sichtbar. Sie haben zwar eine Sicherheitsbeschreibung, jedoch normalerweise eine NULL-SACL. Die Einstellung zwingt den Kernel, diesen Objekten bei ihrer Erstellung eine SACL zuzuweisen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Ein global sichtbares benanntes Objekt, das nicht richtig abgesichert ist, könnte durch ein bösartiges Programm missbraucht werden. Ein Synchronisationsobjekt könnte zum Beispiel durch ein bösartiges Programm zum Absturz gebracht werden. Das Risiko für einen Vorfall ist allerdings gering.

Gegenmaßnahmen

Aktivieren Sie die Einstellung.

Mögliche Auswirkungen

Wenn die Einstellung aktiviert ist, könnte es speziell auf Domänencontrollern und Anwendungsservern sein, dass eine große Zahl von Sicherheitsereignissen erzeugt wird. So könnte die Leistung dieser Systeme verschlechtert werden, oder das Sicherheitsprotokoll wird mit nutzlosen Einträgen gefüllt. Es

gibt leider keine Möglichkeit diese Einträge zu filtern. Auch für Organisationen, die über die Ressourcen zur Analyse diese Einträge verfügen, ist es unwahrscheinlich, dass diese mit den Einträgen etwas anfangen können.

Überwachung: Die Verwendung des Sicherungs- und Wiederherstellungsrechts überprüfen

Diese Sicherheitseinstellung bestimmt, ob die Verwendung sämtlicher Benutzerrechte, einschließlich des Sicherungs- und Wiederherstellungsrechts, überwacht werden soll. Hierzu muss allerdings die Richtlinie **Rechteverwendung überwachen** aktiviert sein. Die Aktivierung dieser Richtlinie könnte eine große Zahl von Sicherheitsereignissen produzieren. Das könnte dazu führen, dass sich die Antwortzeiten der Server verschlechtern, und dass die Ereignisprotokolle mit einer Vielzahl von unwichtigen Ereignissen gefüllt werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Die Aktivierung dieser Einstellung erzeugt einen Eintrag für jede Datei, die gesichert oder wiederhergestellt wird. So können Sie feststellen, ob Administratoren Daten versehentlich oder vorsätzlich wiederherstellen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Die Aktivierung dieser Richtlinie könnte eine große Zahl an Sicherheitsereignissen erzeugen. Dies könnte dazu führen, dass die Antwortzeiten der Server schlechter werden, und dass eine Vielzahl von unwichtigen Ereignissen protokolliert wird.

Überwachung: System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können

Diese Sicherheitseinstellung bestimmt, ob das System heruntergefahren wird, wenn Sicherheitsereignisse nicht protokolliert werden können. Sie ist für Trusted Computer System Evaluation Criteria (TCSEC)-C2 und für die Common-Criteria-Zertifizierung erforderlich, und vermeidet das Auftreten überwachbarer Ereignisse, wenn das System nicht in der Lage ist diese zu protokollieren. Microsoft hat sich zur Unterstützung dieser Anforderung über ein Anhalten des Systems mit einer Stopp-Meldung entschieden. Wenn die Sicherheitsprotokollierung nicht durchgeführt werden kann, und ein Ereignis auftritt, wird bei aktivierter Einstellung daher eine Stopp-Meldung angezeigt. Normalerweise passiert dies, wenn das Sicherheitsprotokoll voll ist und die Aufbewahrungsmethode entweder auf **Nicht überschreiben** oder **Ereignisse nach Tagen überschreiben** konfiguriert ist. Die Stopp-Meldung lautet: *STOP: C0000244 {Fehlgeschlagene Überwachung} Der Versuch einen Überwachungseintrag im Sicherheitsprotokoll zu generieren schlug fehl.*

Zu Wiederherstellung des Systems muss sich ein Administrator anmelden, das Protokoll sichern (optional), und diese Einstellung ändern.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht definiert**

Sicherheitslücken

Wenn der Computer nicht in der Lage ist Sicherheitsereignisse aufzuzeichnen, könnten bei einem Sicherheitsvorfall wichtige Beweise oder Informationen zu Fehlersuche fehlen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Die administrative Belastung durch diese Einstellung ist sehr groß. Vor allem, wenn die Einstellung **Aufbewahrungsmethode des Sicherheitsprotokolls** auf **Nicht überschreiben (Protokoll manuell löschen)** konfiguriert ist. Die zusätzlichen Daten werden durch die Möglichkeit eines DoS-Angriffs (Denial of Service) erkauft. Es könnte nämlich sein, dass der Server durch eine übermäßige Zahl an Anmeldeereignissen oder Sicherheitsereignissen zum Herunterfahren gezwungen wird. Dies könnte außerdem zu einer Beschädigung von Betriebssystem, Anwendungen oder Daten führen.

Geräte: Entfernen ohne vorherige Anmeldung erlauben

Diese Sicherheitseinstellung bestimmt, ob ein tragbarer Computer ohne vorherige Anmeldung abgedockt werden kann. Wenn die Richtlinie aktiviert ist, ist keine Anmeldung erforderlich, und durch Drücken der Auswurftaste an der Hardware kann der Computer abgedockt werden. Wenn die Richtlinie deaktiviert ist, muss sich der Benutzer zum Abdocken des Computers anmelden und über die Berechtigung **Entfernen des Computers von der Dockingstation** verfügen.

> **Anmerkung:** Die Einstellung sollte nur auf tragbaren Computern, die nicht mechanisch abgedockt werden können, aktiviert werden. Ansonsten wird es den Benutzern möglich, den Computer physikalisch zu entfernen, obwohl er sich nicht anmelden kann.

Sicherheitslücken

Wenn die Einstellung aktiviert ist, ist es jedem Angreifer mit physikalischem Zugriff auf den Computer möglich, diesen aus der Dockingstation zu entfernen. Auf Computern, die keine Dockingstation verwenden, hat sie keine Auswirkung.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Gegenmaßnahmen

Deaktivieren Sie die Einstellung.

Mögliche Auswirkungen

Benutzer, deren Computer sich in der Dockingstation befindet, müssen sich anmelden, bevor sie in der Lage sind, diesen zu entfernen.

Geräte: Formatieren und Auswerfen von Wechselmedien zulassen

Diese Einstellung legt fest, wer Wechselmedien formatieren und entfernen kann.

Die möglichen Werte für diese Einstellung sind:

- **Administratoren**
- **Administratoren und Hauptbenutzer**
- **Administratoren und interaktive Benutzer**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten Wechselmedien, die mit NTFS formatiert wurden, auf einen Computer verschieben, auf dem sie Administratorrechte haben. Wenn dies passiert, kann der Benutzer den Besitz jeder Datei übernehmen. Dies gibt ihm dann **Vollzugriff,** und er kann alle Dateien lesen oder ändern. Der Nutzen dieser Option ist gering, da die meisten Wechselmedien recht einfach aus dem Computer entnommen werden können.

Gegenmaßnahmen

Geben Sie das Recht **Auswerfen von NTFS-Wechselmedien zulassen** nur den Administratoren.

Mögliche Auswirkungen

Nur die Administratoren können Wechselmedien, die mit NTFS formatiert wurden, entfernen.

Geräte: Anwendern das Installieren von Druckertreibern nicht erlauben

Damit Sie von einem Computer an einen Netzwerkdrucker drucken können, muss der Treiber für diesen Drucker auf dem lokalen Computer installiert sein. Durch diese Sicherheitseinstellung wird festgelegt, welche Benutzer beim Hinzufügen eines Netzwerkdruckers einen Druckertreiber installieren dürfen. Wurde die Einstellung aktiviert, dürfen nur Administratoren und Hauptbenutzer beim Hinzufügen eines Netzwerkdruckers einen Druckertreiber installieren. Bei deaktivierter Einstellung darf jeder Benutzer beim Hinzufügen eines Netzwerkdruckers einen Druckertreiber installieren.

> **Anmerkung:** Die Einstellung hat keine Auswirkung, wenn ein Administrator für das Herunterladen von Treibern eine vertrauenswürdige Quelle konfiguriert hat. In diesem Fall versucht das Drucker-Subsystem einen Treiber von dieser Quelle herunterzuladen. Wenn dies erfolgreich war, wird der Treiber für den Benutzer installiert. Wenn das Herunterladen fehlschlägt, wird der Treiber nicht installiert und kein Drucker hinzugefügt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Es mag angebracht sein, den Benutzern den Zugriff auf die Drucker ihrer eigenen Arbeitsstation zu gestatten. Dies ist bei Servern jedoch nicht praktikabel. Durch die Installation eines Druckertreibers kann das System ungewollt instabil werden. Nur Administratoren sollen auf Servern dieses Recht haben. Ein Benutzer mit böswilligen Absichten könnte das System beschädigen, indem er einen falschen Treiber installiert. Dies könnte zum Beispiel ein Benutzer sein, der seine Rechte erweitern möchte, um unautorisierten Zugriff auf Daten zu erlangen.

Gegenmaßnahmen

Setzen sie die Einstellung auf den Wert **aktiviert**.

Mögliche Auswirkungen

Nur Administratoren, Hauptbenutzer oder Serveroperatoren können Druckertreiber auf Servern installieren. Wenn die Einstellung aktiviert ist, der Treiber für einen Netzwerkdrucker jedoch schon auf dem Computer existiert, kann der Benutzer den Drucker weiterhin installieren. Die Fähigkeit zur Installation von lokalen Druckern ist von der Einstellung nicht betroffen.

Geräte: Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken

Diese Sicherheitseinstellung bestimmt, ob sowohl lokale als auch Remotebenutzer gleichzeitig auf ein CD-ROM-Laufwerk zugreifen können. Wurde diese Richtlinie aktiviert, dürfen nur die interaktiv angemeldeten Benutzer auf CD-ROMs zugreifen. Wurde diese Richtlinie aktiviert, und kein Benutzer ist interaktiv angemeldet, kann über das Netzwerk auf die CD-ROM zugegriffen werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Der Wert dieser Einstellung ist gering, da sie die Netzwerkbenutzer am Zugriff auf die CD-ROMs hindert, wenn zur selben Zeit ein Benutzer lokal angemeldet ist. CD-ROM Laufwerke werden außerdem nicht automatisch freigegeben. Netzwerkbenutzer sind also nicht in der Lage, auf Daten oder Programme auf CDs zuzugreifen, ohne dass der Administrator dies vorsieht.

Gegenmaßnahmen

Aktivierten Sie die Einstellung.

Mögliche Auswirkungen

Benutzer die sich über das Netzwerk mit einem Server verbinden, sind nicht in der Lage auf ein CD-ROM zuzugreifen solange ein Benutzer lokal angemeldet ist. Auf CD-Servern ist die Einstellung logischerweise nicht zu empfehlen.

Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken

Diese Sicherheitseinstellung bestimmt, ob sowohl lokale als auch Remotebenutzer gleichzeitig auf ein Diskettenlaufwerk zugreifen können. Wurde diese Richtlinie aktiviert, dürfen nur die interaktiv angemeldeten Benutzer auf Disketten zugreifen. Wurde diese Richtlinie deaktiviert und kein Benutzer ist interaktiv angemeldet, kann über das Netzwerk auf die Diskette zugegriffen werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Der Wert dieser Einstellung ist ebenfalls sehr gering, da auch sie die Netzwerkbenutzer nur am Zugriff auf das Diskettenlaufwerk hindert, wenn zur selben Zeit ein Benutzer lokal angemeldet ist. Diskettenlaufwerke werden ebenfalls nicht automatisch freigegeben. Netzwerkbenutzer sind also nicht in der Lage, auf Daten oder Programme auf Disketten zuzugreifen, ohne dass der Administrator dies vorsieht.

Gegenmaßnahmen

Aktivieren Sie die Einstellung.

Mögliche Auswirkungen

Benutzer, die sich über das Netzwerk mit einem Server verbinden, sind nicht in der Lage, auf ein Diskettenlaufwerk zuzugreifen, solange ein Benutzer lokal angemeldet ist.

Geräte: Verhalten bei der Installation von nichtsignierten Treibern

Diese Sicherheitseinstellung bestimmt, was beim Versuch geschieht einen Gerätetreiber, der nicht durch das WHQL (Windows Hardware Quality Lab) getestet wurde, mittels einer Setup-API zu installieren.

Die möglichen Werte für diese Richtlinie sind:

- **Installieren**
- **Warnung, aber Installation zulassen**
- **Installation nicht zulassen**
- **Nicht definiert**

Sicherheitslücken

Diese Option verhindert die Installation von unsignierten Treibern, oder warnt den Administrator davor, dass ein unsignierter Treiber installiert werden soll. Hierdurch wird die Installation von Treibern, die nicht für die Verwendung unter Windows Server 2003 zertifiziert wurden, verhindert. Die Einstellung verhindert keine Angriffe, wie sie zum Beispiel von einigen Angriffstools über manipulierte .sys Dateien durchgeführt werden. Bei solchen Angriffen werden die .sys Dateien als Dienst registriert und gestartet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Warnung, aber Installation zulassen**. Die vorgegebene Einstellung unter Windows Server 2003 ist **Nicht definiert**.

Mögliche Auswirkungen

Benutzer mit ausreichenden Rechten zur Installation von Gerätetreibern sind in der Lage, auch unsignierte Treiber zu installieren. Dies könnte zu Stabilitätsproblemen bei den Servern führen. Ein weiteres potentielles Problem könnten unbeaufsichtigte Installationen sein. Sie werden mit der Einstellung **Warnung, aber Installation zulassen** fehlschlagen.

Domänencontroller: Serveroperatoren das Einrichten von geplanten Tasks erlauben

Diese Sicherheitseinstellung bestimmt, ob Serveroperatoren Aufträge mit Hilfe des AT-Zeitplanungsmechanismus einrichten können.

> **Anmerkung:** Die Einstellung wirkt sich nur auf das Planen von Tasks über den AT-Befehl aus. Der Taskplaner ist nicht betroffen.

Die möglichen Werte für diese Einstellung sind:

- Aktiviert
- Deaktiviert
- Nicht konfiguriert

Sicherheitslücken

Wenn die Einstellung aktiviert ist, werden die Tasks, die von Serveroperatoren über den AT-Befehl erstellt werden, unter dem Sicherheitskontext des Dienstes ausgeführt. Als Standard ist dies das lokale Systemkonto. Das bedeutet, dass Serveroperatoren alles durchführen können, zu dem das lokale Systemkonto in der Lage ist. Sie könnten zum Beispiel ihr Konto zur lokalen Gruppe Administratoren hinzufügen.

Gegenmaßnahmen

Deaktivieren Sie die Einstellung.

Mögliche Auswirkungen

In den meisten Organisationen sollten sich die Auswirkungen in Grenzen halten. Die Benutzer, inklusive der in Gruppe Serveroperatoren, sind auch weiterhin in der Lage den Taskplaner zu

verwenden. Die geplanten Tasks werden im Kontext des Benutzers ausgeführt, der sie geplant hat.

Domänencontroller: Signaturanforderungen für LDAP-Server

Diese Sicherheitseinstellung bestimmt, ob für den LDAP-Server die Signatur mit LDAP-Clients ausgehandelt werden muss.

Die möglichen Werte für diese Einstellung sind:

- **Keine:**
  Eine Signierung der Daten ist nicht erforderlich. Wenn der Client eine Signierung anfordert, wird diese vom Server durchgeführt.
- **Signierung erforderlich:**
  Solange nicht Transport Layer Security/Secure Sockets Layer (TLS/SSL) verwendet wird, muss eine Signierung ausgehandelt werden.
- **Nicht konfiguriert**

Sicherheitslücken

Netzwerkverkehr, der weder signiert noch verschlüsselt ist, ist empfindlich für Man-in-the-middle-Angriffe. Bei dieser Art Angriff fängt ein Eindringling Pakete zwischen Server und Client ab und verändert diese, bevor er sie zum Client weiterleitet. Im Fall eines LDAP-Servers bedeutet das, dass ein Angreifer einen Client mit falschen Einträgen aus dem LDAP-Verzeichnis in die Irre führen könnte. Sie können dieses Risiko verringern, indem Sie strenge physikalische Sicherheitsmaßnahmen zum Schutz Ihrer Netzwerkinfrastruktur ergreifen. Weiterhin können Sie alle Arten von Man-in-the-middle-Angriffe durch die Implementierung der IPSec-Authentifizierung (Internet Protocol Security) im Headermodus (AH – Autentification Header) verhindern, da IPSec eine wechselseitige Authentifizierung und Integritätsprüfung des IP-Verkehrs durchführt.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Signierung erforderlich**.

Mögliche Auswirkungen

Clients, die eine LDAP-Signierung nicht unterstützen, können keine LDAP-Abfragen mehr gegen Domänencontroller durchführen. Das bedeutet, dass auf allen Computern, die in Ihrer Organisation von einem Windows Server 2003 oder Windows XP basierten Computer aus über die Verwendung der Windows NT® Challenge/Response (NTLM) Authentifizierung verwaltet werden, mindesten Windows 2000 Service Pack 3 (SP3) installiert sein muss. Alternativ muss auf diesen Clients die im Microsoft Knowledge Base Artikel Q325465, „*Windows 2000 Domain Controllers Require SP3 or Later When Using Windows.NET Server Administration Tools*“, beschriebene Registrierungsänderung durchgeführt werden. Sie finden den Artikel unter:
http://support.microsoft.com/default.aspx?scid=325465 (englischsprachig).

Domänencontroller: Änderungen von Computerkontenkennwörtern verweigern

Diese Sicherheitseinstellung bestimmt, ob Domänencontroller Anforderungen von Mitgliedscomputern zum Ändern von Computerkontenkennwörtern verweigern.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**

- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Bei aktivierter Einstellung kann ein Domänencontroller *keine* Änderungen am Computerkontenkennwort akzeptieren. Daher bleiben die Passwörter für Angriffe verwundbar.

Gegenmaßnahmen

Deaktivieren Sie die Einstellung.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Domänenmitglied: Daten des sicheren Kanals digital signieren oder verschlüsseln (mehrere Einstellungen)

Die folgenden Einstellungen legen fest, ob ein sicherer Kanal mit einem Domänencontroller aufgebaut werden kann:

- Domänenmitglied: Daten des sicheren Kanals digital signieren (wenn möglich)
- Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln (wenn möglich)
- Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)

Wenn die Einstellung **Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)**aktiviert ist, ist der Aufbau eines sicheren Kanals mit Domänencontrollern, die keine Verschlüsselung oder Signierung unterstützen, nicht möglich.

Um den Authentifizierungsverkehr gegen Man-in-the-middle-Angriffe, Replay-Angriff oder andere Arten von Netzwerkangriffen zu schützen, erstellen Windows-Computer einen sicheren Kommunikationskanal. Dieser Kanal authentifiziert Maschinenkonten und die Benutzerkonten von Remotebenutzern, die sich mit einer Netzwerkressource verbinden wollen.

> **Anmerkung:** Wenn die Einstellung **Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)** auf Mitgliedsservern und –arbeitsstationen aktiviert wird, muss dies auch auf allen Domänencontrollern passieren. Das bedeutet, dass alle Domänencontroller unter Windows NT 4.0 mit Servicepack 6a oder höher ausgeführt werden müssen.

Die möglichen Werte für diese Einstellungen sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn ein Windows Server 2003 System einer Domäne beitritt, wird ein Computerkonto erstellt. Nach dem Domänenbeitritt wird das Passwort dieses Kontos bei jedem Start zum Aufbau eines sicheren Kanals zum Domänencontroller verwendet. Anfragen (zum Beispiel Passwörter), die über diesen

sicheren Kanal gesendet werden, sind authentifiziert und verschlüsselt. Es wird jedoch keine Integritätsprüfung durchgeführt, und es werden nicht alle Informationen verschlüsselt.

Wenn ein System so konfiguriert wird, dass immer verschlüsselt und signiert wird, kann zu einem Domänencontroller, der nicht in der Lage ist den Verkehr zu signieren und zu verschlüsseln, keine Verbindung aufgebaut werden. Wenn die Einstellung nur auf **wenn möglich** konfiguriert ist, kann der Computer zwar einen sicheren Kanal aufbauen, die Verschlüsselung und Signierung wird jedoch vorher ausgehandelt.

Gegenmaßnahmen

- Domänenmitglied: Daten des sicheren Kanals digital signieren (wenn möglich): Aktiviert
- Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln (wenn möglich): Aktiviert
- Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer): Aktiviert

Mögliche Auswirkungen

Der sichere Kanal schützt die Domänen-Anmeldeinformationen, die zum Domänencontroller gesendet werden. Clients, auf denen ältere Betriebssysteme als Windows NT 4.0 mit Servicepack 6a oder Windows 98 mit installiertem DSClient ausgeführt werden, sind nicht mehr in der Lage mit Domänencontrollern zu kommunizieren.

Domänenmitglied: Änderungen von Computerkontenkennwörtern deaktivieren

Die Einstellung legt fest, ob ein Domänenmitglied das Kennwort für sein Computerkonto regelmäßig ändert. Wurde diese Einstellung aktiviert, versucht das Domänenmitglied nicht, das Kennwort für sein Computerkonto zu ändern. Wurde diese Einstellung deaktiviert, versucht das Domänenmitglied das Kennwort für sein Computerkonto gemäß der unter **Domänenmitglied: Maximalalter von Computerkontenkennwörtern** festgelegten Einstellung (standardmäßig alle 30 Tage) zu ändern.

> **Achtung:** Aktivieren Sie diese Einstellung nicht. Passwörter von Computerkonten werden zur Einrichtung von sicheren Kommunikationskanälen zwischen Mitgliedsservern und Domänencontrollern und zwischen den Domänencontrollern selbst verwendet. Über diese sicheren Kanäle werden Informationen für die Authentifizierung und Autorisierung übertragen.

Versuchen Sie nicht über die Verwendung dieser Einstellung und zweier gleicher Computernamen ein Dual-Boot Szenario aufzubauen. Verwenden Sie stattdessen unterschiedliche Computernamen. Die Einstellung wurde entwickelt, um es Organisationen einfacher zu machen, Clients vorzuinstallieren und dieses später in die Produktionsumgebung aufzunehmen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Als Standardkonfiguration für Computer unter Windows Server 2003 die einer Domäne angehören muss das Passwort alle 30 Tage geändert werden. Wenn dies Feature deaktiviert ist, sind die Computer nicht mehr in der Lage ihr Passwort automatisch zu ändern. Hierdurch steigt das Risiko, dass ein Angreifer dieses Passwort herausfindet und missbraucht.

Gegenmaßnahmen

Stellen Sie sicher, dass die Einstellung **deaktiviert** ist.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Domänenmitglied: Maximalalter von Computerkontenkennwörtern

Diese Einstellung legt das maximal erlaubte Alter für das Passwort eines Computerkontos fest. Diese Einstellung wirkt sich auch auf Computer unter Windows 2000 aus, ist aber von diesen Computern aus nicht konfigurierbar.

Die möglichen Werte für diese Einstellung sind:

- **Ein benutzerdefinierter Wert von 0 bis 999 in Tagen.**
- **Nicht konfiguriert**

Sicherheitslücken

In Active Directory-basierten Domänen hat jedes Computerkonto, genau wie alle anderen Konten, ein Passwort. Standardmäßig ändern Domänenmitglieder ihr Passwort alle 30 Tage. Wenn dieser Zeitraum deutlich erhöht wird oder der Wert auf 0 gesetzt wird (das Passwort wird gar nicht mehr geändert), hat ein Angreifer mehr Zeit, um einen Brute-Force-Angriff auf das Passwort eines Computerkontos durchzuführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **30 Tage**.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist. In Organisationen, die ihre Systeme vorinstallieren, um diese dann später zum Beispiel an andere Standorte zu liefern, könnte das Computerpasswort bereits abgelaufen sein. In diesem Fall ist die Maschine dann nicht mehr in der Lage sich an der Domäne zu authentifizieren. Sie müsste wiederhergestellt und erneut in die Domäne aufgenommen werden. Um dies zu verhindern, können Sie zum Beispiel eine spezielle Organisationseinheit für solche Maschinen einrichten und für diese eine größere Zahl an Tagen konfigurieren.

Domänenmitglied: Starker Sitzungsschlüssel erforderlich (Windows 2000 oder höher)

Diese Sicherheitseinstellung bestimmt, ob mit einem Domänencontroller, der nicht in der Lage ist den Verkehr über einen sicheren Kanal mit einem starken 128-Bit Sitzungsschlüssel zu verschlüsseln, ein sicherer Kanal überhaupt etabliert wird. Wenn die Einstellung aktiviert ist, werden in diesem Fall solche Verbindungen gar nicht aufgebaut. Ist sie deaktiviert, dann werden 64-Bit Sitzungsschlüssel für den Aufbau eines sicheren Kanals verwendet.

> **Anmerkung:** Um diese Einstellung auf Arbeitsstationen oder Servern die der Domäne angehören aktivieren zu können, müssen alle Domänencontroller in der Lage sein, einen 128-Bit Schlüssel zu verwenden. Das bedeutet, dass diese unter Windows 2000 oder höher ausgeführt werden müssen.

Die möglichen Werte für diese Richtlinie sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht definiert**

Sicherheitslücken

Sitzungsschlüssel sind in älteren Versionen von Windows nicht so sicher, wie die von Windows Server 2003. Sie sollten diese sichereren Sitzungsschlüssel zum Schutz der Kommunikation über einen sicheren Kanal verwenden, um gegen Eavesdropping- und Session-Hijacking-Angriffe geschützt zu sein. Eavesdropping ist eine Form des Hackens, bei der Durchgangsverkehr im Netzwerk gelesen oder verändert wird. Die Daten können so verändert werden, dass der Absender nicht angezeigt wird, oder die Pakete umgeleitet werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**. Durch Aktivieren dieser Einstellung stellen Sie sicher, dass jeglicher ausgehender Verkehr einen starken Verschlüsselungsschlüssel benötigt. Wenn die Richtlinie deaktiviert ist, wird die Schlüsselstärke mit dem Empfänger ausgehandelt. Diese Option sollte nur aktiviert werden, wenn die Domänencontroller in allen vertrauten Domänen starke Schlüssel unterstützen. Als Voreinstellung ist diese Einstellung deaktiviert.

Mögliche Auswirkungen

Computer, bei denen diese Einstellung aktiviert ist, können Sie in eine Windows NT 4.0 Domäne nicht aufnehmen. Wenn sie auf den Domänencontrollern aktiviert ist, können Computer, die diese Einstellung nicht unterstützen, der Domäne nicht beitreten.

Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen

Diese Sicherheitseinstellung bestimmt, ob der Name des zuletzt am Computer angemeldeten Benutzers auf dem Windows-Anmeldebildschirm angezeigt wird. Wurde diese Richtlinie aktiviert, wird der Name des zuletzt erfolgreich angemeldeten Benutzers im Dialogfeld **Windows-Anmeldung** nicht angezeigt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Ein Angreifer mit Zugriff auf die Konsole, zum Beispiel jemand der physikalischen Zugriff hat, oder jemand der in der Lage ist sich über den Terminaldienst zu verbinden, kann den Namen des zuletzt angemeldeten Benutzers sehen. Der Angreifer könnte dann versuchen sich anzumelden, indem er das Passwort mit Hilfe eines automatisierten Werkzeuges zu erraten versucht.

Gegenmaßnahmen

Setzen Sie die Einstellung **Letzten Benutzernamen nicht im Anmeldedialog anzeigen** auf den Wert

aktiviert.

Mögliche Auswirkungen

Die Benutzer müssen bei jeder Anmeldung an einen Server ihren Benutzernamen eingeben.

Interaktive Anmeldung: Kein STRG+ALT+ENTF erforderlich

Diese Sicherheitseinstellung bestimmt, ob ein Benutzer die Tastenkombination STRG+ALT+ENTF drücken muss, bevor er sich anmelden kann. Wurde diese Richtlinie deaktiviert, muss jeder Benutzer die Tastenkombination STRG+ALT+ENTF drücken, bevor er sich an Windows anmelden kann (es sei denn, für die Windows-Anmeldung wird eine Smartcard verwendet).

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Dieses Feature wurde vom Microsoft zur Unterstützung von Menschen mit Behinderungen entwickelt. Es soll die Anmeldung an Windows vereinfachen. Wenn die Benutzer nicht STRG+ALT+DEL drücken müssen, sind sie anfällig für Angriffe, die auf ein Abfangen des Passwortes abzielen. Das Drücken von STRG+ALT+DEL vor der Anmeldung stellt sicher, dass der Benutzer in einer vertrauenswürdigen Umgebung kommuniziert, wenn er sein Passwort eingibt. Ein Angreifer könnte ein „Trojanisches Pferd“ (ein bösartiges Programm) installieren, das sich wie der Standard Windows-Anmeldebildschirm präsentiert und das Passwort des Benutzers protokolliert. Danach kann der Angreifer sich unter diesem Benutzerkonto anmelden.

Gegenmaßnahmen

Setzen Sie die Einstellung **STRG+ALT+ENTF-Anforderung zur Anmeldung deaktivieren** auf den Wert **deaktiviert**.

Mögliche Auswirkungen

Die Benutzer müssen drei Tasten gleichzeitig drücken, bevor der Anmeldedialog angezeigt wird (es sei denn, Sie nutzen eine Anmeldung durch Smartcards).

Interaktive Anmeldung: Nachricht für Benutzer, die sich anmelden wollen

Diese Sicherheitseinstellung bestimmt die Textnachricht, die Benutzern beim Anmelden angezeigt wird. Diese Einstellung und die Einstellung **Interaktive Anmeldung: Nachrichtentitel für Benutzer die sich anmelden wollen** gehören zusammen. **Interaktive Anmeldung: Nachrichtentitel für Benutzer die sich anmelden wollen** definiert den Titel des Fensters, in dem die Nachricht angezeigt wird. Diese Anmeldenachricht wird normalerweise aus rechtlichen Gründen verwendet, zum Beispiel um Benutzer vor den Folgen des Missbrauchs von Firmeninformationen zu warnen, oder um sie darüber zu informieren, dass ihre Aktionen überwacht werden.

Achtung: Unter Windows XP Professional kann die Anmeldenachricht länger als 512 Zeichen werden und außerdem Zeilenumbrüche enthalten. Windows 2000 Clients können solche Nachrichten nicht anzeigen. Verwenden Sie zur Erstellung von solchen Nachrichten einen

Computer unter Windows 2000. So stellen Sie sicher, dass die Anmeldenachricht auf allen Maschinen korrekt angezeigt wird.

Wenn Sie die Einstellung bereits unter einem Windows XP Computer definiert haben, müssen Sie diese entfernen und unter einem Windows 2000 Computer erneut definieren. Das Ändern der Einstellung unter einem Windows XP Computer reicht nicht aus.

Die möglichen Werte für diese Einstellung sind:

- **Ein benutzerdefinierter Text.**
- **Nicht konfiguriert**

Sicherheitslücken

Öffentliche Untersuchungen der letzten Jahre haben gezeigt, dass Organisationen, die eine Warnmeldung für alle Benutzer, die auf das Netzwerk zureifen wollen anzeigen, eine größere Erfolgsrate bei der Strafverfolgung von Eindringlingen haben, als solche, die dies nicht machen.

Gegenmaßnahmen

Verwenden Sie zum Beispiel den folgenden Text: „Der Zugriff auf dieses System ist nur autorisierten Benutzern gestattet. Nicht autorisierter Zugriff wird strafrechtlich verfolgt. Wenn Sie nicht autorisiert sind, beenden Sie den Zugriff umgehend! Wenn Sie auf OK klicken, akzeptieren Sie diese Vereinbarung“. Für die Einstellung **Nachrichtentitel für Benutzer, die sich anmelden wollen** können Sie zum Beispiel diesen Text verwenden: „Der Zugriff ohne die entsprechende Autorisierung stellt eine Straftat dar.“

Anmerkung: Lassen Sie alle Warnmeldungen, die Sie anzeigen, erst von der Rechts- und Personalabteilung Ihrer Organisation prüfen.

Mögliche Auswirkungen

Die Benutzer sehen ein Dialogfenster, bevor sie in der Lage sind sich auf dem Server anzumelden.

Interaktive Anmeldung: Anzahl zwischenzuspeichernder vorheriger Anmeldungen (für den Fall, dass der Domänencontroller nicht verfügbar ist)

Legt fest, wie oft ein Benutzer sich mit Hilfe zwischengespeicherter Kontoinformationen an einer Windows-Domäne anmelden kann. Alle vorherigen Anmeldeinformationen von Benutzern werden lokal zwischengespeichert, damit sich die Benutzer anmelden können, falls ein Domänencontroller bei nachfolgenden Anmeldeversuchen nicht verfügbar ist. Wenn die Anmeldeinformationen eines Benutzers zwischengespeichert wurden und kein Domänencontroller verfügbar ist, dann wird dem Benutzer die folgende Meldung angezeigt:
Es konnte keine Verbindung zu einem Domänencontroller Ihrer Domäne aufgebaut werden. Sie wurden unter Verwendung von gespeicherten Anmeldeinformationen angemeldet. Die seit Ihrer letzten Anmeldung vorgenommen Profiländerungen stehen möglicherweise nicht zur Verfügung.

Wenn kein Domänencontroller zur Verfügung steht, und für den Benutzer keine Anmeldeinformationen zwischengespeichert sind, dann wird dem Benutzer die folgende Meldung angezeigt:
Das System kann Sie nicht anmelden, da die Domäne <DOMÄNENNAME> nicht zur Verfügung steht.

Die möglichen Werte für diese Einstellung sind:

- **Eine benutzerdefinierte Zahl zwischen 0 und 50**

- **Nicht konfiguriert**

Sicherheitslücken

Die Zahl, die dieser Einstellung zugewiesen wird, ist die Zahl der Benutzer, deren Anmeldeinformationen lokal zwischengespeichert werden. Wenn der Wert auf 10 gesetzt ist, werden die Anmeldeinformationen von 10 Benutzern zwischengespeichert. Wenn sich ein 11. Benutzer anmeldet, wird der älteste zwischengespeicherte Eintrag überschrieben.

Da die Anmeldeinformationen auf dem Server zwischengespeichert werden, könnte ein Angreifer mit Zugriff auf das Dateisystem diese Informationen aufspüren. Er könnte dann über einen Brute-Force-Angriff das Passwort der Benutzer herausfinden.

Diese Art Angriff wird durch die Art, wie Windows Server 2003 diese sensiblen Informationen sichert, verhindert. Die Anmeldeinformationen werden in der Registrierung gespeichert. Diese ist verschlüsselt und über mehrere physikalische Stellen verteilt.

Gegenmaßnahmen

Setzen Sie die Einstellung auf 0. Damit wird die Zwischenspeicherung deaktiviert.

Mögliche Auswirkungen

Benutzer sind nicht in der Lage sich anzumelden, wenn kein Domänencontroller zur deren Authentifizierung zur Verfügung steht. Für Endbenutzersysteme, speziell für Notebookbenutzer, könnten Sie die Einstellung auf 2 setzen. So können diese Benutzer ihr System auch ohne eine Verbindung zum Unternehmensnetzwerk verwenden.

Interaktive Anmeldung: Anwender vor Ablauf des Kennworts zum Ändern des Kennworts auffordern

Legt fest, wie viele Tage im voraus Benutzer darüber informiert werden, dass ihr Kennwort in Kürze abläuft.

Die möglichen Werte für diese Einstellung sind:

- **Eine benutzerdefinierte Zahl Tage zwischen 1 und 999**
- **Nicht konfiguriert**

Sicherheitslücken

Es wird empfohlen, die Passwörter der Benutzer regelmäßig ablaufen zu lassen. Wenn die Benutzer allerdings nicht vor dem Ablauf des Passwortes benachrichtigt werden, bemerken Sie dies vielleicht erst, wenn das Passwort tatsächlich abgelaufen ist. Dies kann dazu führen, dass Netzwerkbenutzer oder Benutzer, die über Wählverbindungen oder VPN-Verbindungen auf das Netzwerk zugreifen, sich nicht mehr am Netzwerk anmelden können.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **14 Tage**.

Mögliche Auswirkungen

Wenn das Passwort in 14 oder weniger Tagen abläuft, sehen die Benutzer bei jeder Anmeldung an der Domäne ein Dialogfenster.

Interaktive Anmeldung: Domänencontrollerauthentifizierung zum Aufheben der Sperrung der Arbeitsstation erforderlich

Zum Entsperren von Computern sind Anmeldeinformationen erforderlich. Diese Sicherheitseinstellung bestimmt bei Domänenkonten, ob zum Aufheben der Sperrung eines Computers die Verbindung zu einem Domänencontroller hergestellt werden muss.

> **Anmerkung:** Diese Einstellung wirkt sich auch auf Computer die Windows 2000 oder höher ausgeführt werden aus. Sie ist jedoch unter Windows 2000 nicht konfigurierbar, sondern nur unter Windows Server 2003.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Der Computer speichert die Anmeldeinformationen jedes authentifizierten Benutzers lokal zwischen. Diese Informationen werden normalerweise bei der Entsperrung des Computers verwendet. In diesem Fall werden kürzlich vorgenommene Änderungen, wie zum Beispiel geänderte Benutzerrechte, Kontosperrungen oder –deaktivierung, beim erneuten Authentifizierungsprozess nicht berücksichtigt und durchgesetzt. So könnte es sein, dass ein Benutzer mit einem deaktivierten Konto weiterhin Zugriff auf das System hat.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Wenn kein Domänencontroller zur Verfügung steht, sind die Benutzer nicht in der Lage ihre Arbeitsstationen zu entsperren.

Interaktive Anmeldung: Smartcard erforderlich

Diese Einstellung legt fest, dass die Benutzer zur Anmeldung eine Smartcard benötigen.

> **Anmerkung:** Die Einstellung wirkt sich zwar auf Windows 2000 Computer aus, ist jedoch über die Verwaltungswerkzeuge auf diesen Computern nicht konfigurierbar.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Durch die Verwendung von Smartcards für die Authentifizierung von Benutzern wird die Sicherheit deutlich verbessert, da es bei ihrer Verwendung für einen Angreifer nahezu unmöglich ist sich mit den heute verfügbaren Technologien einen unberechtigten Zugriff zu verschaffen. Bei der Verwendung von Smartcards wird eine PIN (Personal Identification Numbers) benötigt. So sind für eine Authentifizierung gleich zwei Faktoren erforderlich: Die Smartcard und die PIN. Mit Smartcards ist es für einen Angreifer extrem schwer, den Netzwerkverkehr zwischen dem Computer des Benutzers und dem Domänencontroller zu entschlüsseln. Selbst wenn ihm dies gelingt ist der Nutzen gering, da bei der nächsten Anmeldung ein neuer Sitzungsschlüssel für die Verschlüsselung generiert wird.

Gegenmaßnahmen

Aktivieren Sie die Einstellung.

Mögliche Auswirkungen

Alle Benutzer müssen zur Anmeldung am Netzwerk Smartcards verwenden. Das bedeutet, dass die Organisation eine zuverlässige Public Key Infrastruktur (PKI) aufbauen muss, und allen Benutzer Smartcards und Lesegeräte zur Verfügung gestellt werden müssen. Dies stellt einen erheblichen Aufwand dar, da die Einrichtung dieser Technologien Fachkenntnisse und entsprechende Ressourcen erfordern. Windows Server 2003 stellt allerdings bereits Zertifizierungsdienste zur Verfügung.

Interaktive Anmeldung: Verhalten beim Entfernen von Smartcards

Diese Sicherheitseinstellung bestimmt, was geschieht, wenn die Smartcard für einen angemeldeten Benutzer aus dem Smartcard-Leser entfernt wird.

Die möglichen Werte für diese Richtlinie sind:

- **keine Aktion**
- **Arbeitsstation sperren**
- **abmelden**
- **nicht definiert**

Sicherheitslücken

Wenn Smartcards zur Authentifizierung genutzt werden, sollte der Computer automatisch gesperrt werden, wenn die Karte entfernt wird. Wenn diese Einstellung nicht verwendet wird, könnten Benutzer vergessen die Arbeitsstation zu sperren, wenn sie diese verlassen. Dies könnte böswilligen Benutzern die Möglichkeit geben, auf einen Computer eines anderen Benutzers zuzugreifen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Arbeitsstation sperren**. So wird die Arbeitsstation gesichert, sobald die Smartcard entfernt wird. Der Benutzer kann sich vom Computer entfernen und die Smartcard mitnehmen, wobei jedoch weiterhin eine geschützte Sitzung aufrechterhalten wird. Wenn Sie die Option auf **Abmeldung zwingen** konfigurieren, wird der Benutzer beim Entfernen der Smartcard automatisch abgemeldet.

Mögliche Auswirkungen

Benutzer müssen sich erneut mit ihrer Smartcard und der PIN authentifizieren, wenn sie zu ihrer Arbeitsstation zurückkehren.

Client- und Serverkommunikation digital signieren (mehrere Einstellungen)

Es gibt vier einzelne Einstellungen, die sich auf die digitale Signierung der SMB-Kommunikation beziehen: Clientkommunikation digital signieren (immer), Clientkommunikation digital signieren (wenn möglich), Serverkommunikation digital signieren (immer) und Serverkommunikation digital signieren (wenn möglich).

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht definiert**

Sicherheitslücken

Die digitale Signierung in hochsicheren Netzwerken ist nützlich, um das Angreifen von Server und Clients zu Verhindern. Ein solcher Angriff ist auch als „Session Hijacking“ bekannt – ein Angriff, bei dem der Angreifer eine bestehende Sitzung übernehmen, unterbrechen oder beenden kann. Unsignierte SMB-Pakete könnten von einem Angreifer abgefangen und verändert werden. Ein Angreifer der Zugriff auf das gleiche Netzwerk wie der Client oder Server hat, kann den SMB-Verkehr abfangen. Der Angreifer kann den Verkehr dann verändern und ihn zum Server weiterleiten. Auf diese Art kann es zu unerwünschten Aktionen auf dem Server kommen. Alternativ kann der Angreifer sich - nach einer legitimen Authentifizierung -, selbst als Client oder Server ausgeben und so Zugriff auf sicherheitsrelevante Daten erlangen. Die Signierung authentifiziert beide Seiten. Den Benutzer und den Server, auf dem die Daten gespeichert sind. Wenn der Authentifizierungsprozess auf einer der beiden Seiten fehlschlägt, werden keine Daten übertragen. Wenn die Signierung implementiert ist, verringert sich die Leistung um bis zu 15 Prozent aufgrund der Mehrbelastung durch die Signierung und die Überprüfung. Weitere Informationen über die Signierung entnehmen Sie bitte dem Knowledge Base Artikel Q161372, *How to Enable SMB Signing in Windows NT*.

> **Anmerkung:** Eine alternative Maßnahme, die den Netzwerkverkehr schützen kann, ist die Implementierung von digitalen Signaturen über das IPSec-Protokoll. Es gibt Hardwarelösungen für die IPSec-Verschlüsselung und -Signierung. Diese können genutzt werden, um die Belastung für den Server gering zu halten. Solche Möglichkeiten gibt es bei der SMB-Signierung nicht.

Maßnahmen

Setzen Sie die vier Einstellungen **Clientkommunikation digital signieren (immer), Clientkommunikation digital signieren (wenn möglich), Serverkommunikation digital signieren (immer)** und **Serverkommunikation digital signieren (wenn möglich)** in der allen Server-OUs übergeordneten Gruppenrichtlinie auf den Wert **deaktiviert**.

In manchen Quellen wird vorgeschlagen, diese Einstellungen auf aktiviert zu setzen. Dies kann jedoch zu einer schlechteren Leistung auf Clientcomputern führen und wird die Kommunikation mit älteren SMB-Anwendungen und Betriebssystemen verhindern.

Mögliche Auswirkungen

Das Protokoll für Datei- und Druckfreigabe unter Windows 2000 Server, Windows 2000 Professional und Windows XP Professional, SMB, unterstützt wechselseitige Authentifizierung. Damit werden

„Session Hijacking“ Angriffe abgewehrt, und es werden per Nachrichtenauthentifizierung Active-Message-Angriffe verhindert. SMB führt diese Authentifizierung durch die Platzierung einer digitalen Signatur in jedem SMB durch. Diese wird dann von beiden Seiten, Client und Server, verifiziert.

Wenn der gesamte Verkehr digital signiert wird, wird das auf jeden Fall Auswirkungen auf die Leistung haben. Auf ausgelasteten Servern können diese Auswirkungen substantiell sein. Außerdem können ältere Anwendungen und Betriebssysteme keine Verbindung mehr aufbauen, wenn ein Computer die gesamte unsignierte SMB-Kommunikation ignoriert. Wenn die gesamte SMB-Signierung deaktiviert ist, bleibt der Computer verwundbar für Session-Hijacking-Angriffe.

Microsoft-Netzwerk (Client): Unverschlüsseltes Kennwort an SMB-Server von Drittanbietern senden

Wenn die Einstellung aktiviert ist, ist es dem SMB-Redirector möglich Passworte als Klartext an SMB-Server von Drittanbietern zu senden.

Die möglichen Werte für diese Richtlinie sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht definiert**

Sicherheitslücken

Wenn diese Einstellung aktiviert ist, kann der Server Passwörter an andere Systeme, die den SMB-Dienst ausführen, im Klartext über das Netzwerk übertragen. Diese anderen Systeme können möglicherweise die SMB-Sicherheitsmechanismen von Windows Server 2003 nicht verwenden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Einige sehr alte Anwendungen und Betriebssysteme, wie zum Beispiel MS-DOS, Windows für Arbeitsgruppen 3.11 und Windows 95a, könnten nicht mehr in der Lage sein über das SMB-Protokoll mit den Servern Ihrer Organisation zu kommunizieren.

Microsoft-Netzwerk (Server): Leerlaufzeitspanne bis zum Anhalten der Sitzung

Diese Einstellung legt die Leerlaufzeitspanne fest, nach der eine SMB-Sitzung angehalten wird. Die Sitzung wird bei einer späteren Aktivität des Clients automatisch fortgesetzt.

Der Wert 0 bedeutet bei dieser Einstellung, dass eine Sitzung so schnell wie möglich angehalten wird. Der Maximalwert 99999 (208 Tage) deaktiviert die Einstellung faktisch.

Die möglichen Werte für diese Einstellung sind:

- **Ein benutzerdefinierter Zeitraum in Minuten**
- **Nicht konfiguriert**

Sicherheitslücken

Jede SMB-Sitzung verbraucht Serverressourcen. Wenn eine Vielzahl an Null-Sitzungen aufgebaut wurde, wird der Server langsamer werden oder möglicherweise abstürzen. Ein Angreifer könnte so lange mit hoher Geschwindigkeit SMB-Sitzungen aufbauen, bis der Server nicht mehr antwortet. Der SMB-Dienst wird langsamer werden oder nicht mehr antworten.

Gegenmaßnahmen

Setzen Sie die Einstellung **Leerlaufzeitspanne bis zur Trennung der Sitzung** in der allen Server-OUs übergeordneten Gruppenrichtlinie auf den Wert **15 Minuten**.

Mögliche Auswirkungen

Die Auswirkungen werden minimal sein, da SMB-Sitzungen automatisch neu aufgebaut werden, wenn der Client seine Aktivität wieder aufnimmt.

Netzwerksicherheit: Abmeldung nach Ablauf der Anmeldezeit erzwingen

Diese Einstellung steuert, ob Benutzer, die mit dem lokalen Computer verbunden sind, außerhalb ihrer Anmeldezeiten getrennt werden. Diese Einstellung betrifft die SMB-Komponente eines Windows 2000 Servers. Wenn diese Einstellung aktiviert ist, werden Sub-Sitzungen mit Clients, deren Anmeldezeitraum abgelaufen ist, vom Server gewaltsam getrennt. Wenn diese Einstellung deaktiviert ist, können Clientsitzungen auch nach Ablauf der Anmeldezeit noch weiter bestehen bleiben.

Die möglichen Werte für die Richtlinie sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht definiert**

Sicherheitslücken

Wenn in Ihrer Organisation für die Benutzer Anmeldezeiten definiert sind, dann macht es Sinn, diese Einstellung zu aktivieren.

Gegenmaßnahmen

Aktivieren Sie die Einstellung.

Mögliche Auswirkungen

Wenn in Ihrer Organisation keine Anmeldezeiten verwendet werden, dann hat die Einstellung keine Auswirkungen. Andernfalls werden Benutzersitzungen außerhalb der Anmeldezeiten dieser Benutzer beendet.

Netzwerkzugriff: Anonyme SID-/Namensübersetzung zulassen

Diese Einstellung legt fest, ob anonyme Benutzer SID-Attribute anderer Benutzer erfragen können.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn die Einstellung aktiviert ist, könnte die allgemein bekannte SID des Administratorkontos verwendet werden, um den Namen des Kontos herauszufinden – auch wenn das Konto umbenannt wurde. Mit dem Kontonamen könnte dann zum Beispiel ein Brute-Force-Angriff gegen das Administratorkonto durchgeführt werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Für Mitgliedscomputer ist dies die Standardeinstellung. Daher hat sie hier keine Auswirkung. Die Standardeinstellung für Domänencontroller ist allerdings **aktiviert**. Wenn sie hier deaktiviert ist, bedeutet das, dass ältere Systeme möglicherweise mit einer Windows Server 2003 basierten Domäne nicht mehr kommunizieren können.

Dies betrifft zum Beispiel die folgenden Systeme:

- Windows NT 4.0 basierte RAS-Server.
- Microsoft SQL Server die unter Windows NT 3.x oder Windows NT 4.0 ausgeführt werden.
- RAS-Server und Microsoft SQL Server, die unter Windows 2000 basierten Computern in einer Windows NT 3.x oder Windows NT 4.0 Domäne ausgeführt werden.

Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten nicht erlauben

Diese Einstellung legt fest, welche zusätzlichen Berechtigungen anonyme Verbindungen auf dem Computer besitzen. Windows gestattet anonymen Benutzer diverse Aktivitäten, wie zum Beispiel die Auflistung der Namen aller Domänenkonten und Freigaben. Wenn ein Administrator zum Beispiel für Benutzer Rechte vergeben will, die sich in einer Domäne ohne bidirektionale Vertrauensstellung befinden, ist das sehr praktisch. Normalerweise hat ein anonymer Benutzer dieselben Rechte wie die Gruppe Jeder.

> **Anmerkung:** Auf Domänencontrollern hat diese Einstellung keine Auswirkung.

Unter Windows 2000 wird über die gleichwertige Einstellung mit dem Namen **Zusätzliche Einschränkungen für anonyme Verbindungen** der Registrierungswert *RestrictAnonymous* unter *HKLM\SYSTEM\CurrentControlSet\Control\LSA* verwaltet. Unter Windows Server 2003 wird diese Einstellung durch die beiden Einstellungen **Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten nicht erlauben** und **Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten und Freigaben nicht erlauben** ersetzt. Sie beziehen sich auf die Registrierungswerte *RestrictAnonymousSAM* und *RestrictAnonymous* unter *HKLM\System\CurrentControlSet\Control\Lsa*.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Ein Benutzer, der die Kontennamen abfragen kann, könnte diese für einen Brute-Force-Angriff oder das Ausspähen von Passwörtern (der Benutzer wird vom Angreifer dazu gebracht, sein Passwort bekannt zu geben) verwenden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Es ist nicht mehr möglich Vertrauensstellung zum NT 4.0 basierten Domänen aufzubauen. Außerdem bekommen ältere Clients, wie zum Beispiel Windows NT 3.51 und Windows 95, Probleme beim Zugriff auf Serverressourcen.

Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten und Freigaben nicht erlauben

Diese Einstellung legt fest, welche zusätzlichen Berechtigungen anonyme Verbindungen auf dem Computer besitzen. Windows gestattet anonymen Benutzer diverse Aktivitäten, wie zum Beispiel die Auflistung der Namen aller Domänenkonten und Freigaben. Wenn ein Administrator zum Beispiel für Benutzer Rechte vergeben will, die sich in einer Domäne ohne bidirektionale Vertrauensstellung befinden, ist das sehr praktisch. Normalerweise hat ein anonymer Benutzer dieselben Rechte wie die Gruppe Jeder.

Anmerkung: Auf Domänencontrollern hat diese Einstellung keine Auswirkung.

Unter Windows 2000 wird über die gleichwertige Einstellung mit dem Namen **Zusätzliche Einschränkungen für anonyme Verbindungen** der Registrierungswert *RestrictAnonymous* unter *HKLM\SYSTEM\CurrentControlSet\Control\LSA* verwaltet. Unter Windows Server 2003 wird diese Einstellung durch die beiden Einstellungen **Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten nicht erlauben** und **Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten und Freigaben nicht erlauben** ersetzt. Sie beziehen sich auf die Registrierungswerte *RestrictAnonymousSAM* und *RestrictAnonymous* unter *HKLM\System\CurrentControlSet\Control\Lsa*.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Ein Benutzer, der die Kontennamen abfragen kann, könnte diese für einen Brute-Force-Angriff oder das Ausspähen von Passwörtern (der Benutzer wird vom Angreifer dazu gebracht, sein Passwort bekannt zu geben) verwenden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Es ist nicht mehr mögliche Vertrauensstellung zum NT 4.0 basierten Domänen aufzubauen. Außerdem bekommen ältere Clients, wie zum Beispiel Windows NT 3.51 und Windows 95, Probleme beim Zugriff auf Serverressourcen. Benutzer, die anonym auf Datei- und Druckserver zugreifen, sind nicht mehr in der Lage, die freigegebenen Ressourcen dieser Server anzuzeigen.

Netzwerkzugriff: Speicherung von Anmeldeinformationen oder .NET-Passports für die Netzwerkauthentifikation nicht erlauben

Diese Sicherheitseinstellung bestimmt, ob **Gespeicherte Benutzernamen und Kennwörter**, Anmeldeinformationen oder .NET-Passports für die spätere Verwendung speichern, wenn der Zugriff auf die Domäne authentifiziert wird. Wurde diese Einstellung aktiviert, werden gespeicherte Benutzernamen und Kennwörter am Speichern von Kennwörtern und Anmeldeinformationen gehindert.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Der Benutzer kann auf die auf diese Weise gespeicherten Passwörter zugreifen. Dies kann problematisch sein. Zum Beispiel wenn der Benutzer unwissendlich bösartigen Programmcode ausführt, der diese Passwörter ausliest und an einen nicht autorisierten Benutzer weiterleitet.

> **Anmerkung:** Die Chancen auf eine erfolgreiche Ausnutzung dieser Sicherheitslücke sinken durch die Verwendung einer Anti-Virus Lösung in Verbindung mit durchdachten Richtlinien für Softwareeinschränkungen deutlich. Weitere Informationen über diese Richtlinien finden Sie in *Kapitel 8, Richtlinien für Softwareeinschränkungen*.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Bei der Benutzung ihres Passport-Kontos, oder beim Zugriff auf andere Netzwerkressourcen, auf die sie nicht über ihr Domänenkonto zugreifen können, werden die Benutzer zur Eingabe ihres Passwortes aufgefordert. Die Einstellung wirkt sich nicht auf Webseiten, die eine Anmeldung des Benutzers erfordern aus. Das Speichern von solchen Passwörtern wird über sie nicht verhindert. Sie hat ebenfalls keine Auswirkungen auf den Zugriff auf Netzwerkressourcen über das Active Directory-basierte Domänenkonto des Benutzers.

Netzwerkzugriff: Die Verwendung von 'Jeder'-Berechtigungen für anonyme Benutzer ermöglichen

Diese Sicherheitseinstellung bestimmt, welche zusätzlichen Berechtigungen für anonyme Verbindungen zum Computer erteilt werden. Die Aktivierung dieser Einstellung gibt den Benutzern die Möglichkeit, verschiedenste Aktionen durchzuführen. Zum Beispiel die Auflistung der Namen aller Domänenkonten und Netzwerkfreigaben. Wenn ein Administrator zum Beispiel für Benutzer Rechte

vergeben will, die sich in einer Domäne ohne bidirektionale Vertrauensstellung befinden ist das sehr praktisch. Normalerweise enthält das Token für anonyme Verbindungen die SID der Gruppe Jeder. Daher gelten die Berechtigungen der Gruppe Jeder auch für die anonymen Benutzer.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Ein Benutzer, der die Kontennamen abfragen kann, könnte diese für einen Brute-Force-Angriff oder das Ausspähen von Passwörtern (der Benutzer wird vom Angreifer dazu gebracht, sein Passwort bekannt zu geben) verwenden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Netzwerkzugriff: Named Pipes, auf die anonym zugegriffen werden kann

Diese Sicherheitseinstellung bestimmt, welche Kommunikationssitzungen (Pipes) Attribute und Berechtigungen aufweisen, die einen anonymen Zugriff zulassen.

Die möglichen Werte für diese Einstellung sind:

- **Eine benutzerdefinierte Liste von Freigaben**
- **Nicht konfiguriert**

Sicherheitslücken

Die Beschränkung des Zugriffs über Named Pipes wie COMNAP und LOCATOR verhindert den unautorisierten Zugriff auf das Netzwerk. In der folgenden Tabelle finden Sie eine Liste der Standard-Named-Pipes und ihren Verwendungszweck:

Tabelle 5.1: Standard-Named-Pipes, auf die anonym zugegriffen werden kann

Named Pipe	Zweck
COMNAP	SNA basis Named Pipe - Systems Network Architecture (SNA) ist eine Sammlung von Netzwerkprotokollen, die ursprünglich zur Wartung von IMB-Großrechnern entwickelt wurden.
COMNODE	SNA Server Named Pipe.
SQL\QUERY	Standard Named Pipe für SQL Server.
SPOOLSS	Named Pipe für den Dienst Druckerwarteschlange.
EPMAPPER	Named Pipe für die Zuordnung von Endpunkten.
LOCATOR	Named Pipe für den Dienst Remote Procedure Call Locator.

TrkWks	Named Pipe für den Distributed Link Tracking Client.
TrkSvr	Named Pipe für den Distributed Link Tracking Server.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **NULL**. Das bedeutet, sie wird zwar aktiviert, es werden jedoch keine Named Pipes eingetragen.

Mögliche Auswirkungen

Sie deaktivieren durch diese Konfiguration den Zugriff über Named Pipes und den Zugriff über alle Anwendungen, die diese verwenden.

Der Internet-Maildienst von Microsoft Commercial Internet System 1.0 läuft zum Beispiel unter dem Prozess *Inetinfo.* Inetinfo startet im Kontext des Systemkontos. Wenn der Internet-Maildienst die Microsoft SQL Server-Datenbank abfragen muss, dann verwendet er das Systemkonto. Dieses greift über eine SQL-Pipe auf den Computer zu, auf dem SQL Server ausgeführt wird.

Um solche Probleme zu beheben, lesen Sie bitte den Microsoft Knowledge Base-Artikel 207671: „HOW TO: Access Network Files from IIS Applications“ unter http://support.microsoft.com/default.aspx?scid=207671 (englischsprachig).

Netzwerkzugriff: Registrierungspfade, auf die von anderen Computern aus zugegriffen werden kann

Diese Sicherheitseinstellung bestimmt, auf welche Registrierungspfade über das Netzwerk zugegriffen werden kann.

Die möglichen Werte für diese Einstellung sind:

- **Eine benutzerdefinierte Liste von Registrierungspfaden**
- **Nicht konfiguriert**

Sicherheitslücken

Viele der Informationen in der Registrierung sind sehr sensibel. Ein Angreifer könnte sie zur Durchführung unautorisierter Aktivitäten nutzen. Um dieses Risiko zu verringern wurden der Registrierung ACLs zugewiesen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **NULL** (**Aktiviert**, jedoch ohne Einträge).

Mögliche Auswirkungen

Remoteverwaltungswerkzeuge wie der Microsoft Baseline Security Analyzer und der Microsoft Systems Management Server benötigen einen Remotezugriff auf die Registrierung. Wenn die Standardpfade aus der Liste der zugreifbaren Pfade entfernt werden, funktionieren die und andere Werkzeuge nicht mehr korrekt.

> **Anmerkung:** Wenn Sie den Remotezugriff erlauben möchten, muss der Remoteregistrierungsdienst zusätzlich aktiviert sein.

Netzwerkzugriff: Registrierungspfade und -unterpfade, auf die von anderen Computern aus zugegriffen werden kann

Diese Sicherheitseinstellung bestimmt, auf welche Registrierungspfade und Unterpfade über das Netzwerk zugegriffen werden kann.

Die möglichen Werte für diese Einstellung sind:

- **Eine benutzerdefinierte Liste von Registrierungspfaden**
- **Nicht konfiguriert**

Sicherheitslücken

Viele der Informationen in der Registrierung sind sehr sensibel. Ein Angreifer könnte sie zur Durchführung unautorisierter Aktivitäten nutzen. Um dieses Risiko zu verringern wurden der Registrierung ACLs zugewiesen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf NULL.

Mögliche Auswirkungen

Remoteverwaltungswerkzeuge wie der Microsoft Baseline Security Analyzer und der Microsoft Systems Management Server benötigen einen Remotezugriff auf die Registrierung. Wenn die Standardpfade aus der Liste der zugreifbaren Pfade entfernt werden, funktionieren diese und andere Werkzeuge nicht mehr korrekt.

> **Anmerkung:** Wenn Sie den Remotezugriff erlauben möchten, muss der Remoteregistrierungsdienst zusätzlich aktiviert sein.

Netzwerkzugriff: Named Pipes und Freigaben, auf die anonym zugegriffen werden kann

Wenn die Einstellung aktiviert ist, wird die Zugriff auf alle Freigaben und Pipes verhindert. Die Freigaben und Pipes, die über die Einstellungen **Netzwerkzugriff: Named Pipes, auf die anonym zugegriffen werden kann** und **Netzwerkzugriff: Freigaben, auf die anonym zugegriffen werden kann** definiert sind, sind hiervon nicht betroffen. Die Einstellung fügt dem Registrierungsschlüssel *HKLM\System\CurrentControlSet\Services\LanManServer\Parameters* den Eintrag **RestrictNullSessAccess**=**1** hinzu, und verhindert so den anonymen Zugriff auf Freigaben über NULL-Sessions.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

NULL-Sessions sind eine Schwachstelle die über eine mehrere Freigaben, die auf den Computern Ihrer Umgebung vorhanden sind, ausgenutzt werden kann.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Der Zugriff über NULL-Sessions wird auf alle Freigaben und Pipes, außer auf die der beiden Einstellungen **NullSessionPipes** und **NullSessionShares**, verhindert.

Netzwerkzugriff: Freigaben, auf die anonym zugegriffen werden kann

Diese Sicherheitseinstellung bestimmt, auf welche Netzwerkfreigaben von anonymen Benutzern zugegriffen werden kann.

Die möglichen Werte für diese Einstellung sind:

- **Eine benutzerdefinierte Liste von Freigaben**
- **Nicht konfiguriert**

Sicherheitslücken

Die Aktivierung dieser Gruppenrichtlinieneinstellung ist sehr gefährlich. Jeder Netzwerkbenutzer kann auf alle aufgeführten Freigaben zugreifen. Dies könnte zu einer ungewollten Veröffentlichung oder einer Beschädigung von sensiblen Unternehmensdaten führen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf NULL.

Mögliche Auswirkungen

Die Auswirkungen sollten gering sein, da dies die Standardeinstellung ist.

Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten

Diese Sicherheitseinstellung bestimmt, wie die Authentifizierung von Netzwerkanmeldungen durch lokale Benutzerkonten erfolgt. Wird für diese Option die Einstellung **Klassisch** festgelegt, werden für die Netzwerkanmeldung die lokalen Konteninformationen verwendet. Wenn die Einstellung auf **Nur Gastkonto** konfiguriert ist, werden alle Anmeldungen, die lokale Konten verwenden, automatisch auf das Gastkonto umgeleitet. Das klassische Modell gestattet eine genauere Kontrolle über den Ressourcenzugriff. Sie können mit ihm unterschiedlichen Benutzern unterschiedliche Zugriffe auf Ressourcen ermöglichen. Bei der Verwendung des **Nur Gastkonto**-Modells werden alle Benutzer gleich behandelt. Sie erhalten alle einen Gastzugriff auf die Ressourcen. Auf eigenständigen Windows XP Professional Computern ist die Standardeinstellung **Nur Gastkonto**. Auf Systemen, die einer Domäne angehören, und auf Windows Server 2003 Systemen, ist die Standardeinstellung **Klassisch**.

> **Anmerkung:** Diese Einstellung wirkt sich weder auf Netzwerkanmeldungen mit Domänenkonten, noch auf interaktive Anmeldungen über Telnet oder den Terminaldienst aus.

Wenn der Computer keiner Domäne angehört, werden die Einstellung der Registerkarten **Sicherheit** und **Freigaben** automatisch entsprechend dem gewählten Modell angepasst. Die Einstellung hat auf Windows 2000 Computern keine Auswirkungen.

Die möglichen Werte für diese Einstellung sind:

- **Klassisch – Es werden die lokalen Konten verwendet.**
- **Nur Gastkonto – Lokale Benutzer verwenden das Gastkonto**
- **Nicht konfiguriert**

Sicherheitslücken

Mit dem **Nur Gastkonto**-Modell haben die Benutzer nur Gastzugriff. Das bedeutet, dass sie möglicherweise nicht in der Lage sind in die Freigaben zu schreiben. Obwohl dies die Sicherheit erhöht, könnte es auch bedeuten, dass autorisierte Benutzer nicht mehr auf die gewünschten Ressourcen zugreifen können. Bei Verwendung des klassischen Modells müssen alle lokalen Konten durch Passwörter geschützt werden. Andernfalls hat jeder, der diese Konten verwendet, Zugriff auf die freigegebenen Systemressourcen.

Gegenmaßnahmen

Auf Netzwerkservern setzen Sie die Einstellung auf **Klassisch**. Auf Endbenutzersystemen setzen Sie die Einstellung auf **Nur Gastkonto**.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Netzwerksicherheit: Keine LAN Manager-Hashwerte für nächste Kennwortänderung speichern

Diese Sicherheitseinstellung bestimmt, ob bei der nächsten Kennwortänderung der LAN Manager-Hashwert für das neue Kennwort gespeichert wird.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über einen Angriff auf die SAM könnten Angreifer möglicherweise einen Zugriff auf Benutzernamen und Passworthashes erlangen. Sie könnten das eigentliche Passwort dann über entsprechende Werkzeuge herausfinden. Sobald diese Information zur Verfügung steht, erlangt der Angreifer Zugriff auf Ressourcen Ihres Netzwerkes. Wenn die Einstellung aktiviert wird, werden solche Arten von Angriffen zwar nicht verhindert, aber deutlich erschwert.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**. Es ist unbedingt erforderlich, dass danach alle Benutzer bei ihrer nächsten Netzwerkanmeldung ihr Passwort ändern. Erst dann werden die LAN-Manager Hashes entfernt.

Mögliche Auswirkungen

Ältere Betriebssysteme, wie zum Beispiel Windows 95, Windows 98 und Windows ME, funktionieren nicht mehr korrekt.

Netzwerksicherheit: Abmeldung nach Ablauf der Anmeldezeit erzwingen

Diese Einstellung legt fest, ob Benutzer außerhalb ihrer festgelegten Anmeldezeiten automatisch abgemeldet werden. Sie betrifft alle SMB-Komponenten. Die Sitzungen des Clients mit SMB-Servern werden getrennt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn diese Einstellung deaktiviert ist, könnte ein Benutzer auch über seine Anmeldezeiten hinaus mit einer bestehenden SMB-Sitzung weiter arbeiten.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**. Sie wirkt sich nicht auf Administratorkoten aus.

Mögliche Auswirkungen

SMB-Sitzungen werden auf Mitgliedsservern außerhalb der Anmeldezeiten des Benutzers getrennt. Der Benutzer kann sich außerhalb seiner Anmeldezeiten nicht anmelden.

Netzwerksicherheit: LAN Manager-Authentifizierungsebene

LAN Manager (LM) ist eine ältere Client/Server Software von Microsoft, die es Benutzern gestattet, Computer in einem einzelnen Netzwerk miteinander zu verbinden. Dies umfasst die transparente Datei- und Druckfreigabe, Features zu Benutzersicherheit und Werkzeuge zur Netzwerkverwaltung. In Active Directory Domänen ist Kerberos das Standardprotokoll für die Authentifizierung. Wenn Kerberos aus irgendwelchen Gründen nicht verwendet werden kann, dann wird LM, NTLM oder NTLMv2 verwendet. Die LM-Authentifizierung in den Varianten LM, NT-LM und NT-LM Version 2 (NT-LMv2) wird von allen Windows-Clients als Authentifizierungsprotokoll genutzt. Sie wird zum Beispiel für die folgenden Operationen verwendet:

- Einer Domäne beitreten
- Authentifizierung zwischen Gesamtstrukturen
- Authentifizierung von untergeordneten Domänen
- Authentifizierung von untergeordneten Servern, die nicht auf Windows Server 2003, Windows 2000 oder Windows XP basieren
- Authentifizierung von Servern, die nicht der Domäne angehören

Diese Sicherheitseinstellung bestimmt, welches Anfrage/Antwort-Authentifizierungsprotokoll für Netzwerkanmeldungen verwendet wird. Die Wahl des Protokolls hat auf die Ebene des von Clients

verwendeten Authentifizierungsprotokolls, auf die Ebene der ausgehandelten Sitzungssicherheit und auf die Ebene der vom Server akzeptierten Authentifizierung folgende Auswirkungen:

- **LM- und NT-LM-Antworten senden:** Clients verwenden die LM- und NTLM-Authentifizierung. NTLMv2-Sitzungssicherheit wird nie verwendet. Domänencontroller akzeptieren LM-, NTLM- und NTLMv2-Authentifizierung.
- **LM & NT-LM-Antworten senden (NT-LMv2 Sitzungssicherheit verwenden wenn ausgehandelt):** Clients verwenden die LM- und NTLM-Authentifizierung. NTLMv2-Sitzungssicherheit wird verwendet, wenn der Server diese unterstützt. Domänencontroller akzeptieren LM-, NTLM- und NTLMv2- Authentifizierung.
- **Nur NT-LM-Antworten senden:** Clients verwenden die NTLM-Authentifizierung. Wenn der Server sie unterstützt, wird NTLMv2-Sitzungssicherheit verwendet. Domänencontroller akzeptieren LM-, NTLM- und NTLMv2-Authentifizierung.
- **Nur NT-LMv2-Antworten senden:** Clients verwenden die NTLMv2-Authentifizierung. Wenn der Server sie unterstützt, wird NTLMv2-Sitzungssicherheit verwendet. Domänencontroller akzeptieren LM-, NTLM- und NTLMv2-Authentifizierung.
- **NT-LMv2-Antworten senden (LM verweigern):** Clients verwenden die NTLMv2-Authentifizierung. Wenn der Server sie unterstützt, wird NTLMv2-Sitzungssicherheit verwendet. Domänencontroller akzeptieren ausschließlich NTLMv2-Authentifizierung.

Diese Einstellungen entsprechen den folgenden, in anderen Dokumenten von Microsoft diskutierten, Ebenen:

- **Level 0** – LM- und NT-LM Antworten senden; NT-LMv2-Sicherheit wird nie verwendet. Clients verwenden ausschließlich LM- und NT LM-Authentifizierung. Domänencontroller akzeptieren LM-, NT-LM- und NT-LMv2-Authentifizierung.
- **Level 1** - LM & NT-LM-Antworten senden (NT-LMv2-Sitzungssicherheit verwenden, wenn ausgehandelt). Clients verwenden LM-und NT-LM-Authentifizierung. Wenn der Server dies unterstützt, verwenden Sie NT-LMv2. Domänencontroller akzeptieren LM-, NT-LM- und NT-LMv2-Authentifizierung.
- **Level 2** - nur NT-LM-Antworten senden. Clients verwenden ausschließlich NT-LM-Authentifizierung und verwenden NT-LMv2, wenn der Server dies unterstützt. Domänencontroller akzeptieren LM-, NT-LM- und NT-LMv2-Authentifizierung.
- **Level 3** - nur NT-LMv2-Antworten senden. Clients verwenden NT-LMv2-Authentifizierung und verwenden NT-LMv2-Sitzungssicherheit, wenn der Server dies unterstützt. Domänencontroller akzeptieren LM-, NT-LM- und NT-LMv2-Authentifizierung.
- **Level 4** - NT-LMv2-Antworten senden (LM verweigern). Clients verwenden NT-LMv2-Authentifizierung und NT-LMv2-Sitzungssicherheit, wenn der Server dies unterstützt. Domänencontroller verweigern LM-Authentifizierung und akzeptieren NT-LM- und NT-LMv2-Authentifizierung.
- **Level 5** - NT-LMv2-Antworten senden (LM und NT-LM verweigern). Clients verwenden NT-LMv2-Authentifizierung und NT-LMv2 Sitzungssicherheit, wenn der Server dies unterstützt. Domänencontroller verweigern LM- und NT-LM-Authentifizierung. Sie akzeptieren nur NT-LMv2-Authentifizierung.

Sicherheitslücken

Alle Windows Clients (auch Windows Server 2003, Windows 2000 und Windows XP) senden als Voreinstellung LM- und NT-LM-Authentifizierungsmitteilungen (Ausnahme: Windows 9x Clients – diese senden nur LM). Die vorgegebenen Einstellungen auf Servern ermöglichen es jedem Client sich zu authentifizieren und ihre Ressourcen zu nutzen. Das bedeutet, dass LM-Pakete (das schwächste Authentifizierungsprotokoll) über das Netzwerk gesendet werden. Diese Pakete können von einem Angreifer mitgelesen werden. Der Angreifer hat so eine einfachere Möglichkeit an die Passwörter der Benutzer zu gelangen.

Die Windows 9x und Windows NT Betriebssysteme können das Kerberos V5 Protokoll nicht zur Authentifizierung nutzen. Daher werden als Voreinstellung in einer Windows 2003 Domäne beide Protokolle, LM und NT-LM, zur Authentifizierung verwendet. Sie können mit NT-LMv2 ein sichereres Authentifizierungsprotokoll für Windows 9x und Windows NT durchsetzen. Um den Authentifizierungsprozess zu schützen, nutzt NT-LMv2 einen sicheren Kanal. Wenn Sie NT-LMv2 für ältere Clients nicht einsetzen, werden die Windows 2003 basierten Computer trotzdem das Kerberos V5 Protokoll zur Authentifizierung in einer Windows 2003 Domäne nutzen. Weitere Informationen zur Aktivierung von NT-LMv2 entnehmen Sie bitte dem Knowledge Base Artikel Q239869, „*How to Enable NT-LM 2 Authentication for Windows 95/98/2000/NT."*

Microsoft® Windows NT® 4.0 benötigt Service Pack 4 (SP4), um NT-LMv2 zu unterstützen. Auf Windows 9*x* Plattformen muss erst der Directory Service-Client installiert werden, bevor NT-LMv2 genutzt werden kann.

Gegenmaßnahmen

Setzen Sie die Einstellung **LAN Manager-Authentifizierungsebene** auf **Nur NT-LMv2-Antworten senden**. Wenn alle Clients NT-LMv2 unterstützen, ist dies die von Microsoft und einigen anderen unabhängigen Organisationen vorgeschlagene Authentifizierung.

Mögliche Auswirkungen

Clients, die NT-LMv2 Authentifizierung nicht unterstützen, werden über LM und NT-LM nicht in der Lage sein, sich in der Domäne zu authentifizieren und Ressourcen zu nutzen.

Anmerkung**:** Damit diese Einstellung in einem gemischten Netzwerk mit Systemen unter Windows 2000 und höher und Systemen unter Windows NT 4.0 funktioniert, benötigen Sie einen Hotfix. Sie finden Informationen zu diesem Hotfix im Microsoft Knowledge Base Artikel 305379, „Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain“, unter http://support.microsoft.com/default.aspx?scid=Q305379 (englischsprachig).

Netzwerksicherheit: Signaturanforderungen für LDAP-Clients

Diese Sicherheitsrichtlinie bestimmt das Ausmaß der Datensignatur, die von Clients angefordert wird, die LDAP BIND-Anforderungen ausstellen:

- **Keine:** Die LDAP BIND-Anforderung wird mit den Optionen des Aufrufers ausgeführt.
- **Signierung aushandeln:** Wenn TLS/SSL (Transport Layer Security/Secure Sockets Layer) nicht gestartet wurde, wird die LDAP BIND-Anforderung zusätzlich zu den Optionen des Aufrufers mit der LDAP-Signaturoption aufgebaut. Wenn TLS/SSL gestartet ist, wird die LDAP BIND-Anforderung mit den Optionen des Aufrufers eingerichtet.
- **Signierung erforderlich:** Diese Einstellung entspricht der Einstellung **Signierung aushandeln**. Wenn allerdings die sofortige saslBindInProgress-Antwort des LDAP-Servers nicht angibt, dass eine Signierung erforderlich ist, wird dem Aufrufer mitgeteilt, dass das angeforderte LDAP BIND-Kommando fehlschlägt.

Anmerkung: Diese Einstellung hat keine Auswirkung auf ldap_simple_bind oder ldap_simple_bind_s. Die Microsoft LDAP-Clients verwenden ldap_simple_bind und ldap_simple_bind_s für eine Kommunikation mit Domänencontrollern nicht.

Die möglichen Werte für diese Einstellung sind:

- Keine
- Signierung aushandeln

- Signierung erforderlich
- Nicht konfiguriert
- Sicherheitslücken

Unsignierter Netzwerkverkehr ist durch Man-in-the-middle-Angriffe verwundbar. Im Fall eines LDAP-Servers heißt das, ein Angreifer könnte einem Server falsche LDAP-Antworten vorgaukeln.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Signierung erforderlich**.

Mögliche Auswirkungen

Wenn Sie den Server so konfigurieren, dass LDAP-Signierung erforderlich ist, müssen Sie die Clients genauso konfigurieren. Diese sind sonst nicht in der Lage, mit dem Server zu kommunizieren.

Netzwerksicherheit: Minimale Sitzungssicherheit für NTLM-SSP-basierte Clients (einschließlich sicherer RPC-Clients)

Diese Sicherheitseinstellung ermöglicht es einem Client die Nachrichtenvertraulichkeit (Verschlüsselung), die Nachrichtenintegrität, die 128-Bit-Verschlüsselung oder die NTLMv2-Sitzungssicherheit auszuhandeln.

Die möglichen Werte für diese Einstellung sind:

- **Nachrichtenverschlüsselung erforderlich** - Die Verbindung schlägt fehl, wenn keine Verschlüsselung ausgehandelt werden kann.
- **Nachrichtensignierung erforderlich** - Die Verbindung schlägt fehl, wenn keine Signierung ausgehandelt werden kann.
- **128-Bit Verschlüsselung erforderlich** - Die Verbindung schlägt fehl, wenn keine 128-Verschlüsselung ausgehandelt werden kann.
- **NTLMv2 Sitzungssicherheit erforderlich** - Die Verbindung schlägt fehl, wenn keine NTLMv2-Sitzungssicherheit ausgehandelt werden kann.
- **Nicht konfiguriert**.

Sicherheitslücken

Die Aktivierung aller Optionen dieser Einstellung verhindert, dass ein Angreifer dem Netzwerkverkehr, der den NTLM Security Support Provider (NTLM SSP) verwendet, Informationen entnimmt. So schützt diese Einstellung gegen Man-in-the-middle-Angriffe.

Gegenmaßnahmen

Aktivieren Sie alle vier Optionen dieser Einstellung.

Mögliche Auswirkungen

Clientcomputer, die diese Einstellungen verwenden, sind nicht mehr in der Lage mit älteren Servern die diese nicht unterstützen zu kommunizieren.

Netzwerksicherheit: Minimale Sitzungssicherheit für NTLM-SSP-basierte Clients (einschließlich sicherer RPC-Server)

Diese Sicherheitseinstellung ermöglicht es einem Server, die Nachrichtenvertraulichkeit (Verschlüsselung), die Nachrichtenintegrität, die 128-Bit-Verschlüsselung oder die NTLMv2-Sitzungssicherheit auszuhandeln.

Die möglichen Werte für diese Einstellung sind:

- **Nachrichtenverschlüsselung** erforderlich – Die Verbindung schlägt fehl, wenn keine Verschlüsselung ausgehandelt werden kann.
- **Nachrichtensignierung erforderlich** – Die Verbindung schlägt fehl, wenn keine Signierung ausgehandelt werden kann.
- **128-Bit Verschlüsselung erforderlich** - Die Verbindung schlägt fehl, wenn keine 128-Verschlüsselung ausgehandelt werden kann.
- **NTLMv2-Sitzungssicherheit erforderlich** - Die Verbindung schlägt fehl, wenn keine NTLMv2-Sitzungssicherheit ausgehandelt werden kann.
- **Nicht konfiguriert**.

Sicherheitslücken

Die Aktivierung aller Optionen dieser Einstellung verhindert, dass ein Angreifer dem Netzwerkverkehr, der den NTLM Security Support Provider (NTLM SSP) verwendet, Informationen entnimmt. So schützt diese Einstellung gegen Man-in-the-middle-Angriffe.

Gegenmaßnahmen

Aktivieren Sie alle vier Optionen dieser Einstellung.

Mögliche Auswirkungen

Clientcomputer, die diese Einstellungen verwenden, sind nicht mehr in der Lage mit diesem Computer zu kommunizieren.

Wiederherstellungskonsole: Automatische administrative Anmeldungen zulassen

Diese Sicherheitseinstellung bestimmt, ob das Kennwort für das Administratorkonto angegeben werden muss, bevor der Zugriff auf das System gewährt wird. Wurde diese Option aktiviert, fordert die Wiederherstellungskonsole kein Kennwort an, und die Anmeldung am System erfolgt automatisch.

Die möglichen Werte für diese Richtlinie sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht definiert**

Sicherheitslücken

Die Wiederherstellungskonsole kann zur Reparatur eines Systems, das nicht gestartet werden kann, sehr nützlich sein. Die automatische Anmeldung zu aktivieren kann allerdings gefährlich sein. Jeder

kann am Server die Stromversorgung unterbrechen, den Server neu starten und die Wiederherstellungskonsole auswählen. Damit hat diese Person dann vollen Zugriff auf das System.

Gegenmaßnahmen

Setzen Sie die Einstellung **Wiederherstellungskonsole: Automatische administrative Anmeldungen zulassen** auf **deaktiviert**.

Mögliche Auswirkungen

Die Benutzer müssen bei der Verwendung der Wiederherstellungskonsole einen Namen und ein Kennwort eingeben.

Wiederherstellungskonsole: Kopieren von Disketten und Zugriff auf alle Laufwerke und alle Ordner zulassen

Durch Aktivieren dieser Sicherheitsoption wird der SET-Befehl der Wiederherstellungskonsole verfügbar. Dieser ermöglicht die Festlegung der folgenden Umgebungsvariablen der Wiederherstellungskonsole:

- **AllowWildCards:** Aktiviert die Unterstützung von Platzhalterzeichen für bestimmte Befehle (zum Beispiel den DEL-Befehl).
- **AllowAllPaths:** Ermöglicht den Zugriff auf alle Dateien und Ordner auf dem Computer.
- **AllowRemovableMedia:** Ermöglicht das Kopieren von Dateien auf auswechselbaren Datenträgern (zum Beispiel Disketten).
- **NoCopyPrompt:** Unterdrückt die Anzeige einer Bestätigungsaufforderung beim Überschreiben einer vorhandenen Datei.

Die möglichen Werte für diese Richtlinie sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht definiert**

Sicherheitslücken

Ein autorisierter Administrator könnte vergessen eine CD-ROM oder eine Diskette mit sensiblen Daten zu entfernen. Ein böswilliger Benutzer könnte diese entwenden. Ein autorisierter Administrator könnte versehentlich eine Startdiskette im Computer vergessen. Wenn der Computer dann aus irgendeinem Grund neu startet und das BIOS zum booten von CD-ROM oder Diskette konfiguriert ist, startet der Server von der Diskette. Das könnte dazu führen, dass der Server im Netzwerk nicht mehr zu Verfügung steht.

Gegenmaßnahmen

Setzen Sie die Einstellung **Wiederherstellungskonsole: Kopieren von Disketten und Zugriff auf alle Laufwerke und alle Ordner zulassen** auf **deaktiviert**.

Mögliche Auswirkungen

Benutzer, welche die Wiederherstellungskonsole verwenden, sind nicht in der Lage auf Dateien oder Ordner auf Disketten zuzugreifen.

Herunterfahren: Herunterfahren des Systems ohne Anmeldung zulassen

Diese Sicherheitseinstellung bestimmt, ob ein Computer ohne vorherige Anmeldung heruntergefahren werden kann. Wenn sie deaktiviert ist, steht der Befehl *Herunterfahren* im Anmeldebildschirm nicht zur Verfügung. In diesem Fall muss sich der Benutzer am Computer anmelden können und das Recht **System herunterfahren** haben um den Computer herunterfahren zu können.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer, die lokal oder über den Terminaldienst Zugriff auf die Konsole haben, können das System herunterfahren. Ein Angreifer oder ein fehlgeleiteter Benutzer könnte sich mit dem Server über den Terminaldienst verbinden und könnte ihn herunterfahren oder neu starten, ohne ihn oder sich selbst zu authentifizieren. Ein Angreifer könnte diese Aktion auch durchführen, wenn er lokal Zugriff auf die Konsole hat. Ein Server, der neu gestartet wird, führt zu einem zeitweiligen DoS-Zustand. Die Anwendungen und Dienste eines heruntergefahrenen Servers stehen nicht mehr zu Verfügung.

Gegenmaßnahmen

Setzen Sie den Wert **Herunterfahren des Systems ohne Anmeldung zulassen** für die Gruppenrichtlinie der OU, die allen Servern übergeordnet ist, auf **deaktiviert**.

Mögliche Auswirkungen

Administratoren müssen sich am Server anmelden, wenn sie ihn herunterfahren oder neu starten möchten.

Herunterfahren: Auslagerungsdatei des virtuellen Arbeitspeichers löschen

Diese Sicherheitseinstellung bestimmt, ob die Auslagerungsdatei des virtuellen Arbeitsspeichers gelöscht wird, sobald das System heruntergefahren wird. Wenn Speicherbereiche nicht verwendet werden, werden sie in die Auslagerungsdatei auf der Festplatte ausgelagert. Auf einem laufenden System ist diese Auslagerungsdatei exklusiv durch das Betriebssystem geöffnet. Damit die Auslagerungsdatei nicht über den Start eines anderen Betriebssystems ausgelesen werden kann, sollte sie beim Herunterfahren des Systems gelöscht werden. Wurde diese Richtlinie aktiviert, wird die Systemauslagerungsdatei beim Herunterfahren gelöscht. Außerdem wird die Ruhezustanddatei (**hiberfil.sys**) genullt, sofern der Ruhezustand auf einem tragbaren Computer deaktiviert wurde.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wichtige Informationen im Speicher werden regelmäßig in Auslagerungsdatei geschrieben. Dies hilft Windows Server 2003 bei der Handhabung von Multitaskingfunktionen. Ein Angreifer, der physikalischen Zugriff auf den heruntergefahrenen Server hat, könnte auf den Inhalt der Auslagerungsdatei zugreifen. Der Angreifer verschiebt die Festplatte in einen anderen Computer und analysiert dann den Inhalt der Auslagerungsdatei. Dieser Vorgang erfordert viel Zeit. Es könnten jedoch Daten, die im RAM zwischengespeichert wurden, in falsche Hände geraten.

Anmerkung: Ein Angreifer mit physikalischem Zugriff auf den Server könnte diese Gegenmaßnahme umgehen, indem er einfach die Stromzufuhr unterbricht.

Gegenmaßnahmen

Setzen Sie die Einstellung **Auslagerungsdatei des virtuellen Arbeitspeichers beim Herunterfahren des Systems löschen** in der allen Server-OUs übergeordneten Gruppenrichtlinie auf den Wert **aktiviert**. Windows Server 2003 löscht dann beim Herunterfahren die Auslagerungsdatei. Abhängig von der Größe der Auslagerungsdatei kann es einige Minuten dauern, bis das System vollständig heruntergefahren ist.

Mögliche Auswirkungen

Besonders auf Servern mit einer großen Auslagerungsdatei wird das Herunterfahren länger dauern. Bei einem Server mit 2 GB RAM und einer Auslagerungsdatei von 2 GB kann das Herunterfahren 20, 30 oder mehr Minuten länger dauern. In einigen Organisationen ist eine solche Verzögerung beim Herunterfahren vielleicht aufgrund einer Serverlevel-Vereinbarung nicht möglich. Daher sollten Sie vorsichtig sein, wenn sie diese Einstellung in Ihrer Umgebung implementieren.

Systemkryptografie: Starken Schlüsselschutz für auf dem Computer gespeicherte Benutzerschlüssel erzwingen

Diese Sicherheitseinstellung bestimmt, ob für die privaten Schlüssel von Benutzern, zum Beispiel die S-MIME Schlüssel, ein Kennwort verwendet werden muss.

Die möglichen Werte für diese Einstellung sind:

- **Keine Eingabe erforderlich**
- **Eingabe bei der ersten Verwendung erforderlich**
- **Eingabe bei jeder Verwendung erforderlich**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn diese Richtlinie aktiviert ist, muss der Benutzer bei jeder Verwendung eines Schlüssels ein Passwort eingeben. Hierdurch wird es für einen Angreifer schwerer auf die lokal gespeicherten Schlüssel eines Benutzers zuzugreifen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Eingabe bei jeder Verwendung erforderlich**.

Mögliche Auswirkungen

Die Benutzer müssen bei jedem Zugriff auf einen gespeicherten Schlüssel ihr Passwort eingeben. Zum Beispiel bei der Signierung einer E-Mail durch ein S-MIME Zertifikat. Wenn Ihnen der Aufwand, der mit dieser Konfiguration verbunden ist, zu hoch ist, sollten Sie die Einstellung mindestens auf **Eingabe bei der ersten Verwendung erforderlich** konfigurieren.

Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden

Diese Sicherheitseinstellung bestimmt, ob der TLS/SSL-Sicherheitsanbieter (Transport Layer Security/Secure Sockets Layer) nur die Verschlüsselungssammlung TLS_RSA_WITH_3DES_EDE_CBC_SHA unterstützt. Für die für TLS-Verkehr nur die Triple Data Encryption Standard (DES)-Verschlüsselung verwendet, für den TLS-Schlüsselaustausch und die Authentifizierung wird der Rivest-Shamir-Adleman (RSA) Public Key-Algorithmus verwendet und für das TLS-Hashing wird nur der Secure Hash Algorithm Version 1 (SHA1) Hashalgorithmus verwendet. Für EFS (Encrypting File System – Verschlüsselndes Dateisystem) wird ausschließlich die Triple-DES- Verschlüsselung verwendet. Standardmäßig verwendet EFS den DESX-Algorithmus (eine Variation des DES-Algorithmus).

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Durch die Aktivierung dieser Richtlinie stellen Sie sicher, dass die Computer Ihrer Umgebung für die digitale Verschlüsselung, Signierung und das Hashen den stärksten verfügbaren Schlüssel verwenden. Hierdurch wird das Risiko einer Kompromittierung von verschlüsselten oder signierten Daten durch einen nicht autorisierten Benutzer verringert.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Clients mit dieser Einstellung sind möglicherweise nicht mehr in der Lage verschlüsselt oder signiert mit Server zu kommunizieren, die diese Algorithmen nicht unterstützen. Viele Apache-basierte Webserver unterstützen TLS zum Beispiel nicht. Wenn Sie diese Einstellung aktivieren, müssen Sie den Internet Explorer ebenfalls für die Verwendung von TLS konfigurieren.

► Um den Internet Explorer für die Verwendung von TLS zu konfigurieren
Aktivieren Sie auf der Registerkarte **Erweitert** der **Internetoptionen** des Internet Explorers die Option **TLS1.0 verwenden**.

Es ist außerdem möglich, diese Option über eine Gruppenrichtlinie oder über das Internet Explorer Administrationskit zu konfigurieren.

Systemobjekte: Standardbesitzer für Objekte, die von Mitgliedern der Administratorengruppe erstellt werden

Diese Einstellung legt fest, ob die Gruppe Administratoren oder der Ersteller eines Objektes der

Standardbesitzer des erstellten Objektes wird.

Die möglichen Werte für diese Einstellung sind:

- **Administratoren**
- **Objekt-Ersteller**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn die Einstellung auf **Administratoren** gesetzt ist, sind andere Benutzer nicht in der Lage Besitzer von neuen Objekten zu werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Objekt-Ersteller**.

Mögliche Auswirkungen

Wenn Systemobjekte erstellt werden, wird der Ersteller des Objektes auch dessen Besitzer.

Systemobjekte: Groß-/Kleinschreibung für auf anderen Betriebssystemen basierende Subsysteme ignorieren

Diese Sicherheitseinstellung bestimmt, ob für alle Subsysteme durchgesetzt wird, dass die Groß- und Kleinschreibung erzwungen wird. Im Win32-Subsystem wird die Groß- und Kleinschreibung nicht berücksichtigt. Der Kernel unterstützt jedoch die Berücksichtigung der Groß- und Kleinschreibung für andere Subsysteme, zum Beispiel für POSIX.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Da Windows nicht zwischen Groß- und Kleinschreibung unterscheidet (POSIX Subsysteme unterscheiden dies), ist es für einen Benutzer dieses Subsystems möglich eine Datei zu erstellen, die den gleichen Dateinamen trägt, wie eine weitere Datei, indem er für den Dateinamen Groß- und Kleinbuchstaben mischt. Hierdurch könnte ein anderer Benutzer am Zugriff auf die Datei über die normalen Win32-Werkzeuge gehindert werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Alle Subsysteme ignorieren die Groß- und Kleinschreibung. Benutzer, die UNIX basierte

Betriebssysteme gewohnt sind, könnten hierdurch verwirrt werden.

Systemobjekte: Standardberechtigungen interner Systemobjekte (zum Beispiel symbolischer Verknüpfungen) verstärken

Diese Sicherheitseinstellung bestimmt die Stärke der standard- Zugriffsliste (Discretionary Access Control List, DACL) für Objekte. Windows 2000 pflegt eine globale Liste von freigegebenen Systemressourcen, wie zum Beispiel DOS-Geräten, über die Objekte über Prozesse hinweg gesucht und verwendet werden können.

Die möglichen Werte für diese Richtlinie sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht definiert**

Sicherheitslücken

Jedes Objekt wird mit einer vorgegebenen DACL erstellt. Diese legt fest, wer das Objekt mit welchen Rechten verwenden kann. Wenn diese Richtlinie aktiviert ist, wird die vorgegebene DACL stärker abgesichert. Sie erlaubt dann Nicht-Administratoren nur das Lesen, nicht aber das Ändern, der nicht von ihnen erstellten Objekte.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Systemeinstellungen: optionale Subsysteme

Diese Sicherheitseinstellung bestimmt, welche Subsysteme für die Unterstützung Ihrer Anwendungen verwendet werden.

Die möglichen Werte für diese Einstellung sind:

- **Eine benutzerdefinierte Liste der Subsysteme**
- **Nicht konfiguriert**

Sicherheitslücken

Das POSIX-Subsystem ist ein Electrical and Electronic Engineers (IEEE) -Standard. Er definiert eine Gruppe von Betriebssystemdiensten. Es gibt ein Sicherheitsrisiko bei diesem Subsystem. Wenn ein Benutzer einen Prozess startet und sich dann abmeldet, dann kann der nächste angemeldete Benutzer unter bestimmten Umständen auf diesen Prozess zugreifen. Da dieser Prozess möglicherweise die Systemprivilegien des ersten Benutzers enthält, könnte dies ein Sicherheitsproblem darstellen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **NULL**. Dies ist auch der Standardwert.

Mögliche Auswirkungen

Anwendungen, die vom POSIX-Subsystem abhängig sind, funktionieren nicht mehr.

Systemeinstellungen: Zertifikatsregeln zur Durchsetzung von Softwareeinschränkungsrichtlinien auf Windows-Programme anwenden

Diese Einstellung legt fest, ob bei einem Start einer .exe-Datei eine Verarbeitung von digitalen Zertifikaten durchgeführt wird. Sie aktiviert oder deaktiviert Zertifikatsregeln (eine Variante der Softwareeinschränkungsregeln). Mit diesen Softwareeinschränkungsregeln können Sie Zertifikatsregeln erstellen, die das Ausführen von Software erlauben oder verweigern, die mit Authenticode® signiert ist.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Softwareeinschränkungsrichtlinien schützen Benutzer und Computer vor der Ausführung von nicht autorisiertem Programmcode.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Wenn die Einstellung aktiviert ist, kann die Leistung beim Start von signierter Software schlechter werden.

6

Ereignisprotokolle

Über diese Einstellungen können Sie das Verhalten des Anwendungs-, Sicherheits- und Systemprotokolls konfigurieren. Die Standardeinstellungen finden Sie in der mitgelieferten Excel-Tabelle *Windows Standardeinstellungen für Sicherheit und Dienste.xls.*

Sie finden die Einstellungen unter dem folgenden Pfad:
Computerkonfiguration\Windows Einstellungen\Sicherheitseinstellungen\Ereignisprotokoll\Einstellungen der Ereignisprotokolle

Maximale Größe für das Anwendungs-, Sicherheits- und Systemprotokoll

Obwohl es möglich ist, diese Werte über die Gruppenrichtlinie oder das Snap-In Ereignisanzeige auf bis zu vier Gigabyte zu setzten, gibt es einige Faktoren, welche die effektive Größe der Protokolle sehr viel kleiner machen.

Der Ereignisprotokoll-Dienst wird unter dem Prozess services.exe als eventlog.dll ausgeführt. Die Protokolldateien werden immer komplett geladen. Unter Windows kann aber kein Prozess mehr als ein Gigabyte Speicher nutzen. Das bedeutet, dass sich alle Dienste, die unter dem Prozess services.exe ausgeführt werden, ein Gigabyte Speicher teilen müssen. Der freie Speicher wird in 64-Kilobyte Blöcken zugewiesen. Wenn, unabhängig von der konfigurierten Größe der Protokolldateien, kein freier Speicher mehr zu Verfügung steht, ist der Dienst nicht mehr in der Lage, Ereignisse zu protokollieren. Außerdem könnte es zur Fragmentierung des entsprechenden Speichers und so zu deutlichen Leistungseinbrüchen kommen.

Daher liegt die tatsächlich mögliche Größe für alle Ereignisprotokolle zusammen bei maximal einem Gigabyte. Tests bei Microsoft haben ergeben, dass eine praktikable Größe auf den meisten Servern bei ca. 300 Megabyte für alle Protokolle zusammen liegt. Auf Domänencontrollern sollten Sie bedenken, dass zu diesem Wert auch noch das DNS-Protokoll und das Replikationsprotokoll hinzukommen. Diese Einschränkungen haben bei einigen Kunden zu Problemen geführt. Zu ihrer Lösung sind jedoch grundlegende Änderungen an der Architektur der Ereignisprotokolle nötig. Microsoft möchte diese in der nächsten Version von Windows vornehmen.

Da es keine einfache Berechnung für die beste Protokollgröße für einen Server gibt, müssen Sie diese selbst ermittelt. Jeder Protokolleintrag ist ca. 500 Bytes groß, und die Protokollgröße muss ein Vielfaches von 64 KB betragen. Verwenden Sie die durchschnittliche Zahl von Ereignissen pro Tag zusammen mit diesen Werten, um die beste Protokollgröße zu ermitteln. Eine Beispielrechnung: Ihr Dateiserver generiert ca. 5.000 Einträge pro Tag, und Sie möchten mindestens die Einträge der letzten vier Wochen zur Verfügung haben. Die Protokollgröße muss ca. 70 MB betragen (500 Byte * 5.000 Einträge/Tag * 28 Tage = 70.000.000 Byte). Prüfen Sie den Server in den nächsten vier Wochen regelmäßig und passen Sie die Protokollgröße bei Bedarf an.

Die möglichen Werte für diese Einstellungen sind:

- Ein benutzerdefinierter Wert in Kilobyte zwischen **64** und **4.194.240**. Dieser muss durch 64 teilbar sein.

Sicherheitslücken

Wenn Sie die Anzahl der Objekte, die Sie in Ihrer Organisation überwachen, deutlich erhöhen, laufen Sie Gefahr, dass das Sicherheitsprotokoll bis zu seiner maximalen Kapazität vollgeschrieben wird. Dies führt zu einem Herunterfahren des Systems. Wenn das passiert, ist das System nicht nutzbar, bis

ein Administrator das Systemprotokoll geleert hat. Um dies zu vermeiden, deaktivieren Sie die in Kapitel 5, Sicherheitsoptionen, beschriebene Einstellung **Überwachung: System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können** und erhöhen Sie die Protokollgröße.

Gegenmaßnahmen

Auf allen Computern in Ihrer Organisation sollen so sensible Überwachungsrichtlinien aktiv sein, dass legitime Benutzer für Ihre Aktionen zur Verantwortung gezogen werden können und nicht autorisierte Aktivitäten entdeckt und verfolgt werden können.

Mögliche Auswirkungen

Wenn die Ereignisprotokolle voll sind, können keine neuen Einträge hineingeschrieben werden. Es sei denn, die Aufbewahrungsmethode ist so gewählt, dass das System die ältesten Einträge mit den neusten überschreibt.

Die Konsequenz dieser Einstellung ist, dass die älteren Ereignisse aus dem Protokoll verschwinden. Angreifer könnten dies zu ihrem Vorteil nutzen, indem sie eine große Anzahl belangloser Einträge erzeugen, um die Beweise für den Angriff zu überschreiben.

Im Idealfall werden alle speziell überwachten Ereignisse an einen Server mit Microsoft® Operations Manager (MOM) oder einem anderen Überwachungswerkzeug gesendet. Dieser Punkt ist ganz besonders wichtig, denn ein Angreifer, der erfolgreich in den Server eingedrungen ist, könnte das Ereignisprotokoll löschen. Wenn jedoch alle Ereignisse an einen Überwachungsserver gesendet werden, sind Sie in der Lage, Informationen über die Aktivitäten des Angreifers abzufragen.

Lokalen Gastkontozugriff auf Ereignisprotokolle verhindern

Diese Sicherheitseinstellung bestimmt, ob Gastbenutzer am Zugriff auf das Anwendungsereignisprotokoll gehindert werden.

Standardmäßig verbietet Windows Server 2003 Gästen den Zugriff auf alle Systeme. Daher hat diese Einstellung keinen wirklichen Effekt auf Standardsysteme.

> **Anmerkung:** Diese Einstellung gibt es im lokalen Richtlinienobjekt eines Computers nicht.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

> **Anmerkung:** Diese Einstellung gibt es in der lokalen Richtlinie nicht. Sie betrifft nur Computer unter Windows 2000 und höher.

Sicherheitslücken

Ein Angreifer, der sich erfolgreich mit Gastrechten am Computer angemeldet hat, könnte über das Ereignisprotokoll wichtige Systeminformationen herausfinden. Mit diesen könnte er weitere Angriffe vorbereiten.

Gegenmaßnahmen

Setzen Sie die Einstellung für alle drei Protokolle auf **Aktiviert**.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Ereignisprotokolle aufbewahren

Diese Einstellung legt fest, wie viele Tage die Protokolle aufbewahrt werden.

Die möglichen Werte für diese Einstellung sind:

- Ein benutzerdefinierter Wert in Tagen zwischen 1 und 365.
- Nicht konfiguriert.

Anmerkung: Diese Einstellung gibt es in der lokalen Richtlinie nicht.

Sicherheitslücken

Stellen Sie sicher, dass die Einstellung so groß ist, dass sie die Protokolle vor dem Überschreiben von Einträgen sichern können.

Gegenmaßnahmen

Setzen Sie die Einstellung für alle Protokolle auf **Nicht konfiguriert**.

Mögliche Auswirkungen

Keine, da dies die Standardeinstellung ist.

Aufbewahrungsmethode für das Anwendungs-, Sicherheits- und Systemprotokoll

Diese Einstellung legt die Aufbewahrungsmethode für die Protokolle fest. Wenn Sie diese nicht archivieren möchten, verwenden Sie die Option **Ereignisse bei Bedarf Überschreiben**. Andernfalls wählen Sie **Ereignisse auf Tagen basieren überschreiben** und definieren die gewünschte Anzahl an Tagen für die Einstellung **Protokoll Aufbewahrungsdauer**. Wenn Sie sichergehen möchten, dass keine Einträge verloren gehen, wählen Sie die Einstellung **Ereignisse nicht überschreiben (Protokoll manuell aufräumen)**. Mit dieser werden allerdings keine neuen Einträge mehr in die Protokolle geschrieben, wenn diese voll sind.

Die möglichen Aufbewahrungsmethoden sind:

- Ereignisse auf Tagen basieren überschreiben
- Ereignisse bei Bedarf überschreiben
- Ereignisse nicht überschreiben (Protokoll manuell aufräumen)
- Nicht konfiguriert

Anmerkung: Diese Einstellung steht in der lokalen Richtlinie nicht zur Verfügung.

Sicherheitslücken

Wenn Sie die Anzahl der Objekte, die Sie in Ihrer Organisation überwachen, deutlich erhöhen, laufen Sie Gefahr, dass das Sicherheitsprotokoll bis zu seiner maximalen Kapazität vollgeschrieben wird. Dies führt zu einem Herunterfahren des Systems. Wenn das passiert ist, das System nicht nutzbar, bis ein Administrator das Systemprotokoll geleert hat. Um dies zu vermeiden deaktivieren Sie die Einstellung **Überwachung: System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können** und erhöhen die Protokollgröße. Wenn die Einstellung auf **Ereignisse auf Tagen basieren überschreiben** oder **Ereignisse nicht überschreiben (Protokoll manuell aufräumen)** konfiguriert ist, könnte dies zum Verlust wichtiger Ereignisse, oder zu einem DoS-Zustand führen.

Gegenmaßnahmen

Setzen Sie die Einstellung **Aufbewahrungsmethode für das Systemprotokoll** auf **Überschreiben wenn nötig**. Oft wird vorgeschlagen diese Einstellung auf manuell zu konfigurieren. Tatsächlich ist der administrative Aufwand, den man sich mit dieser Einstellung auferlegt, zu groß für die meisten Organisationen. Im Idealfall werden alle wichtigen Ereignisse an einen Überwachungsserver mit MOM oder einem anderen automatischen Überwachungswerkzeug gesendet.

Mögliche Auswirkungen

Wenn die Ereignisprotokolle voll sind, können keine neuen Einträge hineingeschrieben werden. Es sei denn, die Aufbewahrungsmethode ist so gewählt, dass das System die ältesten Einträge mit den neuesten überschreibt.

Zugriffsrechte auf die Protokolle delegieren

Unter Microsoft Windows Server 2003 ist es möglich die Berechtigungen für den Zugriff auf die Protokolle anzupassen. In vorherigen Versionen war dies nicht möglich. Einige Organisationen möchten bestimmten Mitgliedern des IT-Teams möglicherweise nur einen Lesezugriff auf die Protokolle gewähren. Deren Zugriffskontrollliste wird als Security Descriptor Definition Language (SDDL) ß-Zeichenkette in einen Registrierungsschlüssel mit der Bezeichnung *CustomSD* gespeichert. Eine Beispielkonfiguration könnte so aussehen:

Erstellen Sie unter *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\CustomSD* einen REG_SZ Registrierungswert mit dem Wert *O:BAG:SYD:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG)(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x5;;;SO)(A;;0x1;;;IU)(A;;0x1;;;SU)(A;;0x1;;;S-1-5-3)(A;;0x2;;;LS)(A;;0x2;;;NS)*

Starten Sie den Computer neu, damit die Einstellung wirksam wird.

> **Achtung:** Bei der Bearbeitung von Registrierungswerten sollten sie vorsichtig sein, da es keine "Undo"-Funktion gibt. Wenn Sie bei der Bearbeitung einen Fehler machen, müssen Sie diesen per Hand beheben. Außerdem könnten Sie die ACLs der Protokolle versehendlich so konfigurieren, dass niemand mehr auf diese Zugreifen kann. Gehen Sie sicher, dass Sie die SDDL vollständig verstanden haben, bevor Sie Änderungen vornehmen. Testen Sie alle Änderungen sorgfältig, bevor Sie diese in Ihre Produktionsumgebung übernehmen.

Weitere Informationen zur Konfiguration der Protokoll-Zugriffsrechte unter Windows Server 2003 finden Sie im Dokument *How to: Set Event Log Security Locally or by Using Group Policy in Windows Server 2003* unter http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b323076 (englischsprachig).

Weiter Informationen zu SDDL finden Sie im Dokument *Security Descriptor Definition Language* unter http://msdn.microsoft.com/library/default.asp?url=/library/en-

us/security/Security/security_descriptor_definition_language.asp (englischsprachig).

7

Systemdienste

Die Systemdienste werden anders als die anderen Einstellungen beschrieben, da Sicherheitslücken, Gegenmaßnahmen und mögliche Auswirkungen grundsätzlich für alle Dienste identisch sind. Wenn Sie Microsoft® Windows Server 2003 installieren, werden verschiedene Dienste so konfiguriert, dass sie automatisch beim Systemstart gestartet werden. Es ist möglich, dass Sie in Ihrer Organisation einige dieser Dienste gar nicht benötigen. Sie wurden jedoch trotzdem mit aufgenommen. Zum Beispiel, um die Anwendungs- oder Clientkompatibilität sicherzustellen oder die Systemverwaltung zu ermöglichen. Die mit diesem Handbuch gelieferte Excel-Tabelle, *Windows Standardeinstellungen für Sicherheit und Dienste.xls,* zeigt Ihnen die Standard-Starttypen der Systemdienste.

Übersicht

Ein Dienst muss sich für einen Zugriff auf Ressourcen und Objekte des Betriebssystems über ein Konto anmelden. Die meisten Dienste sind so entworfen worden, dass das von ihnen verwendete Konto nicht geändert werden kann. Eine Änderung dieses Kontos könnte zu einer Fehlfunktion dieser Dienste führen. Wenn Sie ein Konto verwenden, dass nicht über die Berechtigung verfügt sich als Dienst anzumelden, wird diesem Konto über das Snap-In *Dienste* automatisch das Recht zum Anmelden als Dienst zugewiesen. Dies garantiert allerdings noch nicht, dass der Dienst auch gestartet werden kann. Unter Windows Server 2003 gibt es drei lokale Standardkonten, die von verschiedenen Diensten zur Anmeldung verwendet werden:

- **Lokales Systemkonto:** Das lokale Systemkonto ist ein Konto mit umfangreichen Rechten. Es hat vollständigen Zugriff auf das System und führt Netzwerkoperationen für den Computer durch. Wenn sich ein Dienst auf einem Domänencontroller über das lokale Systemkonto anmeldet, hat dieser Dienst Zugriff auf die gesamte Domäne. Einige Dienste melden sich als Voreinstellung über das lokale Systemkonto an. Ändern Sie diese Standardeinstellung nicht. Der Name des Kontos lautet *System*. Es hat kein Passwort.
- **Lokales Dienstkonto:** Das lokale Dienstkonto ist ein spezielles systemeigenes Konto, das einem authentifizierten Benutzerkonto entspricht. Es hat die gleichen Zugriffsberechtigungen auf Ressourcen und Objekte wie die Mitglieder der Gruppe Benutzer. Durch diesen eingeschränkten Zugriff wird Ihr System vor kompromittierten Diensten oder Prozessen geschützt. Dienste, die das lokale Dienstkonto für einen Netzwerkzugriff auf Ressourcen verwenden, führen dieses anonym über eine NULL-Session durch. Der Name des Kontos lautet *Lokaler Dienst.* Das Konto hat kein Passwort.
- **Netzwerk Dienstkonto:** Das Netzwerk-Dienstkonto ist ein spezielles systemeigenes Konto, das einem authentifizierten Benutzerkonto entspricht. Es hat die gleichen Zugriffsberechtigungen auf Ressourcen und Objekte wie die Mitglieder der Gruppe Benutzer. Durch diesen eingeschränkten Zugriff wird Ihr System vor kompromittierten Diensten oder Prozessen geschützt. Dienste, die das Netzwerk-Dienstkonto für einen Netzwerkzugriff auf Ressourcen verwenden, führen dieses über das Computerkonto durch. Der Name des Kontos lautet Netzwerkdienst. Es hat kein Passwort.

Wichtig: Eine Änderung der Standardeinstellungen der Dienste könnte zu Fehlern bei Schlüsseldiensten führen. Speziell bei Diensten, deren Starttyp auf *Automatisch* konfiguriert ist, sollten Sie bei Änderungen von Starttyp und verwendetem Konto Vorsicht walten lassen.

Sicherheitslücken

Jeder Dienst und jede Anwendung ist ein potentieller Angriffspunkt. Daher sollten Sie alle nicht benötigten Dienste und ausführbaren Dateien aus Ihrer Systemumgebung entfernen. Es gibt unter

Windows Server 2003 weitere, optionale Dienste. Zum Beispiel die Zertifikatsdienste, die bei einer Standardinstallation nicht installiert werden. Sie können diese optionalen Dienste auf einem bestehenden System über die Option Software der Systemsteuerung, den Windows Server 2003 Serverkonfigurationsassistenten oder über eine angepasste automatische Installation installieren. In der *Mitgliedsserver Basisrichtlinie* sind diese optionalen Dienste, wie alle anderen nicht benötigten Dienste auch, deaktiviert.

> **Wichtig:** Wenn Sie zusätzliche Dienste aktivierten, könnten diese von weiteren Diensten abhängig sein. Fügen Sie alle Dienste hinzu, die für die entsprechende Serverrolle notwendig sind.

Gegenmaßnahmen

Deaktivierten Sie alle nicht benötigten Dienste.

Die möglichen Werte für die Einstellung des jeweiligen Dienstes sind:

- **Automatisch**
- **Manuell**
- **Deaktiviert**
- **Nicht Konfiguriert**

Sie können Sicherheitseinstellungen der Dienste außerdem über die jeweiligen ACL anpassen.

Mögliche Auswirkungen

Die Deaktivierung einiger Dienste, zum Beispiel der Sicherheitskontenverwaltung, führt dazu, dass das System nicht mehr gestartet werden kann. Die Deaktivierung anderer kritischer Dienste kann dazu führen, dass sich das System nicht mehr an einem Domänencontroller authentifizieren kann. Für alle Dienste gilt, dass bei ihrer Deaktivierung alle von dem Dienst abhängigen Dienste nicht mehr ausgeführt oder gestartet werden können.

Wenn Sie mit der Deaktivierung von Diensten experimentieren, testen Sie die Einstellung erst auf einem Nicht-Produktivsystem.

Sie können die Einstellungen der Systemdienste über den folgenden Pfad konfigurieren: *Computerkonfiguration\Windows Einstellungen\Sicherheitseinstellungen\Systemdienste*

Beschreibung der einzelnen Dienste

Dieser Abschnitt beschreibt die einzelnen Dienste von Windows Server 2003. Es werden sowohl die zusätzlich installierbaren, als auch die Standarddienste beschrieben.

Warndienst

Der Warndienst benachrichtigt ausgewählte Benutzer und Computer bei administrativen Alarmen. Über ihn können Sie Benutzern, die mit ihrem Netzwerk verbunden sind, Alarmmeldungen senden. Alarmmeldungen sollen Benutzer vor Sicherheits-, Zugriffs- und Sitzungsproblemen warnen. Sie werden als Nachrichten vom Server an den Computer des Endbenutzers geschickt. Um Nachrichten empfangen zu können, muss der Nachrichtendienst auf dem Computer des Benutzers ausgeführt werden. Wenn der Warndienst deaktiviert wird, sind Anwendungen, welche die NetAlertRaise oder NetAlertRaiseEx APIs (Application Programming Interfaces) verwenden, nicht mehr in der Lage Benutzer oder Computer zu benachrichtigen. Viele Verwaltungswerkzeuge für unterbrechungsfreie Stromversorgungen (USVs) verwenden den Warndienst, zum Beispiel um Administratoren über

Ereignisse zu informieren.

Gatewaydienst auf Anwendungsebene

Dieser Dienst ist eine Unterkomponente des Internet Connection Sharing (ICS)/Internet Connection Firewall (ICF)-Dienstes. Er gibt unabhängigen Softwareanbietern die Möglichkeit, Protokoll-Plugins zu schreiben, die es ihren proprietären Netzwerkprotokollen erlauben, die Firewall zu passieren und hinter ICS zu arbeiten. Plug-ins für den Gatewaydienst sind in der Lage Ports zu öffnen und Daten auszutauschen. In Windows Server 2003 ist das einzige vorhandene Plug-in das für das File Transfer Protocol (FTP). Wenn der Dienst angehalten wird, steht für diese Protokolle keine Netzwerkverbindung mehr zu Verfügung. Außerdem starten alle von diesem Dienst abhängigen Dienste nicht mehr. Anwendungen, wie zum Beispiel der MSN® Messenger, können nicht mehr ausgeführt werden..

Anwendungsverwaltung

Dieser Dienst bietet Softwareinstallationsdienste, wie zum Beispiel Zuweisen, Veröffentlichen und Entfernen. Der Dienst führt Anfragen aus, die Programme auflisten, installieren und entfernen. Wenn Sie auf **Software** in der Systemsteuerung klicken und der Computer einer Domäne angehört, dann ruft das Programm über diesen Dienst eine Liste der zur Installation verfügbaren Programme ab. Er ist außerdem für die Installation oder Entfernung von Anwendungen, für Anwendungsanfragen zu Dateiendungen und für Anfragen zu COM-Klassen (Component Object Model) und ProgIDs, die auf dem Computer nicht vorhanden sind zuständig. Der Dienst wird beim ersten Aufruf gestartet und wird, wenn er einmal gestartet wurde, nicht wieder beendet.

> **Anmerkung:** Weitere Informationen zu COM, COM-Klassen und ProgIDs finden Sie im Software Development Kit (SDK) der MSDN® Bibliothek unter http://www.microsoft.com/windows/reskits/webresources (englischsprachig).

Wenn der Dienst angehalten oder deaktiviert wird, sind die Benutzer nicht mehr in der Lage, über Active Directory verteilte Anwendungen zu installieren, entfernen oder anzuzeigen. Im Dialogfenster **Neue Anwendungen über das Netzwerk installieren** wird die Meldung *Es stehen keine Programme zu Installation zur Verfügung* angezeigt. Sobald der Dienst gestartet wurde, ist es nicht möglich ihn anzuhalten. Um zu verhindern, dass er gestartet wird, müssen Sie ihn deaktivieren.

ASP .NET Statusdienst

Dieser Dienst stellt eine Unterstützung für den Sitzungsstatus außerhalb von Prozessen für ASP.NET zur Verfügung. ASP.NET verwendet Sitzungsstati – über den Parameter **Session** der ASP.NET-Seiten steht eine Liste der Werte einer Clientsitzung zur Verfügung. Für die Speicherung dieser Sitzungsdaten gibt es drei Optionen: Im Prozess, Microsoft SQL Server Datenbank und außerhalb des Prozesses über den Session State Server. Der ASP.NET State Service speichert die Sitzungsdaten außerhalb des Prozesses. Der Dienst kommuniziert über Sockets mit ASP.NET das auf dem Webserver ausgeführt wird. Wen er angehalten oder deaktiviert wird, werden die Anfragen zu Sitzungsdaten nicht beantwortet.

Automatische Aktualisierung

Dieser Systemdienst ermöglicht das Herunterladen und Installieren von kritischen Windows-Updates. Sie brauchen nicht manuell nach kritischen Updates zu suchen – das Betriebssystem holt diese direkt auf Ihren Computer. Es erkennt, wenn Sie Ihre Internetverbindung verwenden und sucht über den Windows Update-Dienst automatisch nach anwendbaren Updates. Abhängig von der von Ihnen konfigurierten Einstellung, benachrichtig der Dienst Sie entweder vor dem Herunterladen oder vor der Installation, oder er installiert die Updates automatisch für Sie. Sie können das Feature **Automatisches Update** über die Option **System** der **Systemsteuerung** deaktivieren. Außerdem können Sie über eine administrative Vorlage einen Internet-Server definieren, der den Software

Update Service ausführt und so Updates zur Verfügung stellt. Der Update-Client fragt dann diesen Server nach anwendbaren Updates. Weitere Informationen zu Software Update Services finden Sie auf der entsprechenden Webseite unter http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp (englischsprachig).

Wenn der Dienst angehalten oder deaktiviert wird, werden kritischen Updates nicht mehr automatisch heruntergeladen. Das Suchen, Herunterladen und Installieren dieser Updates muss von Ihnen über die Windows Update Webseite unter http://windowsupdate.microsoft.com (englischsprachig) manuell durchgeführt werden.

Intelligenter Hintergrundübertragungsdienst

Dieser Dienst (auch **Background Intelligent Transfer Service** – **BITS** genannt) ist für die asynchrone Übertragung von Dateien zwischen Client und HTTP-Server zuständig. Normalerweise werden BITS-Anfragen und der Dateitransfer über freie Netzwerkbandbreite durchgeführt. Daher sind andere netzwerkbezogene Aktivitäten nicht betroffen. BITS hält die Übertragung an, wenn die Verbindung getrennt wird oder wenn der Benutzer sich abmeldet. Die BITS-Verbindung ist allerdings anhaltend. Dateitransfers werden von BITS über eine Warteschlange durchgeführt. Sie können den Übertragungen in dieser Warteschlange Prioritäten zuweisen und definieren, ob eine Vordergrund- oder Hintergrundübertragung durchgeführt werden soll. Hintergrundübertragungen sind optimaler, da BITS hier die nicht verwendete Netzwerkbandbreite nutzt. Wenn eine Anwendung dann mehr Bandbreite verwendet, verringert BITS die Übertragungsrate automatisch.

BITS stellt eine Prioritätsebene für die Vordergrundübertragung und drei Ebenen für die Hintergrundübertragung zur Verfügung. Die hohe Priorität hat Vorrang. Wenn es Aufträge mit gleicher Priorität gibt, teilen sich diese die Übertragungszeit. Ein Round-Robin-Verfahren stellt sicher, dass große Aufträge die Warteschlange nicht komplett blockieren. Aufträge mit niedriger Priorität werden erst ausgeführt, wenn alle Aufträge mit hoher Priorität abgearbeitet oder fehlerhaft sind.

Wenn **BITS** auf manuell gesetzt ist, kann der Dienst auf Anforderung gestartet werden. Wenn dann alle Aufträge durchgeführt wurden, wird der BITS-Dienst wieder angehalten.

Wenn der Dienst angehalten wird, sind Features wie zum Beispiel das automatische Update nicht mehr in der Lage Downloads durchzuführen. Auch der Empfang von Updates über SUS funktioniert nicht mehr. Wenn der Dienst deaktiviert ist, können alle Dienste, die von diesem abhängig sind, keine Dateiübertragung mehr durchführen. Es sei denn, sie haben einen Sicherungsmechanismus, der es ihnen ermöglicht, einen Transfer über andere Wege, zum Beispiel den Internet Explorer, durchzuführen.

Zertifikatsdienste

Dieser Dienst ist ein Teil des Betriebssystemkerns, der es Unternehmen ermöglicht, als eigenständige Zertifizierungsstelle (Certification Authority - CA) aufzutreten und eigene digitale Zertifikate, zum Beispiel für SSL, EFS, IPSec oder eine Smartcardanmeldung, auszugeben. Windows Server 2003 bietet mehrere CA-Hierarchieebenen, Gegenzertifizierungen und Online- und Offline-CAs. Wenn der Zertifikatsdienst angehalten oder beendet wird, werden keine Zertifikatsanforderungen mehr beantwortet. Widerrufslisten (Certificate Revocation Lists - CRLs) und Delta-CRLs werden nicht mehr veröffentlicht. Wenn der Dienst so lange angehalten ist, dass die CRLs ablaufen, können bestehende Zertifikate nicht mehr bestätigt werden.

Client Service für Netware

Dieser Dienst bietet Benutzern, die mit ihm interaktiv auf einem Server angemeldet sind, Zugriff auf Datei- und Druckressourcen in NetWare-Netzwerken. Mit dem Clientdienst für Netware können Sie auf Datei- und Druckressourcen auf Netware-Servern unter Novell Directory Services (NDS) oder Bindery (NetWare Versionen 3.x oder 4.x) zugreifen. Er unterstützt das IP-Protokoll nicht und kann in einer IP-Umgebung und zur Kommunikation mit NetWare 5.x nicht verwendet werden. Hierfür müssen Sie auf

dem NetWare 5.x Server das Internetwork Packet Exchange (IPX) Protokoll verwenden oder einen Redirector nutzen, der mit dem Netware Core Protocol (NCP) kompatibel ist. Wenn der Dienst beendet oder deaktiviert wird, verlieren Sie den Zugriff auf Datei- und Druckressourcen in NetWare-Netzwerken.

Ablagemappe

Dieser Dienst ermöglicht es der Ablagemappe Daten für Remotebenutzer zur Verfügung zu stellen. Er ist vom Network Dynamic Data Exchange (NetDDE)-Dienst für die Erstellung von Freigaben abhängig. Wenn der Dienst deaktiviert wird, werden alle Dienste, die von diesem abhängig sind, nicht gestartet. Clipbrd.exe kann jedoch weiterhin zu Anzeige der lokalen Ablagemappe verwendet werden.

Clusterdienst

Dieser Dienst steuert Servercluster und verwaltet die Clusterdatenbank. Ein Cluster ist ein Zusammenschluss vom unabhängigen Computer, der als einzelner Computer verwendet werden kann. Die Verwaltung eines Clusters kann sehr kompliziert sein. Der **Cluster Service** verteilt Daten und Rechenzeit auf die Knoten des Clusters. Wenn ein Knoten ausfällt, übernehmen andere Knoten die Daten und Dienste des ausgefallenen Knotens. Wenn ein Knoten hinzugefügt oder repariert wird, weist der **Cluster Service** diesem Knoten Daten und Rechenzeit zu.

Unter der Windows-Plattform gibt es für unterschiedliche Anwendungstypen zwei unterschiedliche Clusterlösungen: Servercluster und Network Load Balancing (NLB)-Cluster. Servercluster bieten Anwendungen, wie zum Beispiel Datenbanken oder Dateiservern, über einen Failover eine hochverfügbare Umgebung. NLB-Cluster ermöglichen eine hochverfügbare und skalierbare Umgebung für Anwendungen, wie zum Beispiel Webserver. Sie verteilen Clientanfragen über eine Gruppe identischer Server. Dieser Dienst ist eine grundlegende Softwarekomponente, die alle Aspekte der Servercluster-Aktivitäten und die Clusterdatenbank kontrolliert. Jeder Knoten eines Clusters führt eine Instanz des Clusterdienstes aus.

Unter Windows Server 2003 sind bis zu acht Knoten pro Cluster möglich. Ein Cluster kann jedoch nur Knoten unter Enterprise Server oder unter Datacenter Server enthalten. Möglich ist es aber, einen gemischten Cluster mit Windows 2000 Knoten und Windows Server 2003 Knoten zu betreiben.

Servercluster können in drei unterschiedlichen Konfigurationen eingerichtet werden:

- **Einzelner Knoten:** Solche Servercluster können mit oder ohne externe Speichergeräte konfiguriert werden. Wenn kein externes Speichergerät zur Verfügung steht, wird die lokale Festplatte als Clusterspeichergerät konfiguriert. Sie können die Einzelknoten-Konfiguration zum Beispiel für die Entwicklung von Clusteranwendungen nutzen.
- **Einzelnes Quorum:** Diese Servercluster haben zwei oder mehr Knoten. Sie sind so konfiguriert, dass jeder Knoten mit einem oder mehreren Clusterspeichergeräten verbunden ist. Die Konfigurationsdaten des Clusters sind auf einem einzelnen Clusterspeichergerät, Quorum-Platte genannt, gespeichert.
- **Mehrfacher Knotensatz:** Diese Servercluster bestehen aus zwei oder mehr Knoten. Die Knoten können, müssen jedoch nicht mit einem oder mehren Clusterspeichergeräten verbunden sein. Die Konfigurationsdaten des Clusters sind auf mehreren Platten des gesamten Clusters gespeichert. Der Clusterdienst stellt sicher, dass diese Daten über alle Platten hinweg konsistent gehalten werden.

COM+ Ereignissystem

Dieser Dienst ermöglicht die automatische Verteilung von Ereignissen an COM-Komponenten. Er erweitert das COM+ Programmiermodel. Statt ständig den Server abfragen zu müssen, benachrichtigt er das Ereignissystem, wenn eine Information verfügbar ist. Wenn der Dienst angehalten wird, steht die Systemereignisbenachrichtung nicht mehr zu Verfügung. Anmelde- und Abmeldenachrichten

werden nicht mehr angezeigt.

COM+ Systemanwendung

Dieser Dienst verwaltet die Konfiguration und Verfolgung von COM+ basierten Komponenten. Die meisten COM+ basierten Komponenten funktionieren nicht mehr, wenn er angehalten wird.

Computer Browser

Dieser Dienst führt eine aktuelle Liste aller Computer im Netzwerk und stellt diese Programme zur Verfügung. Er wird von Windows-basierten Computern verwendet und ist zum Anzeigen von Domänen und Ressourcen notwendig. Computer, die als Suchdienst agieren, pflegen eine Liste aller freigegebenen Ressourcen des Netzwerkes. Ältere Windows-Anwendungen, wie zum Beispiel NET VIEW und der Windows NT® Explorer, benötigen diesen Dienst. Unter Windows 95 wird die angezeigte Liste der Netzwerkressourcen zum Beispiel über den Computer abgerufen, der als Hauptsuchdienst agiert. Außer diesem Hauptsuchdienst gibt es noch einige weitere Rollen, die ein Computer im Netzwerk ausführen kann. Diese Rollen können unter bestimmten Umständen wechseln. Wenn der Dienst angehalten wird, steht die Ressourcenliste nicht mehr zu Verfügung.

Kryptografiedienste

Dieser Dienst stellt Schlüsselverwaltungsdienste zur Verfügung und setzt sich aus drei verschiedenen Diensten zusammen:

- **Catalog Database Service:** Dieser Dienst ist für das Hinzufügen, Entfernen und Anzeigen von Katalogdateien verantwortlich. Katalogdateien werden zur Signierung der Betriebssystemdateien verwendet. Der Dienst wird vom Windows Dateischutz, der Treibersignierung und dem Setup verwendet. Er kann während des Setups nicht angehalten werden. Wenn er nach dem Setup angehalten wird, wird er auf Anforderung neu gestartet. Wenn dies nicht möglich ist, sind Systemdateischutz und Treibersignierung nicht mehr in der Lage Signaturen zu prüfen.
- **Protected Root Service:** Dieser Dienst ist für das Hinzufügen und Entfernen von Zertifikaten der Stammzertifizierungsstelle zuständig. Er zeigt das Dialogfenster mit dem Zertifikatsnamen an. Wenn Sie dort OK anklicken, wird das Zertifikat zur Liste der vertrauenswürdigen Stammzertifizierungsstellen hinzugefügt. Nur das lokale Systemkonto hat auf diese Liste Schreibzugriff. Wenn der Dienst angehalten wird, dann ist es nicht mehr möglich Zertifikate vertrauenswürdiger Stammzertifizierungsstellen hinzuzufügen oder zu entfernen.
- **Key Service:** Dieser Dienst gestattet es Administratoren Zertifikate anstelle des Computerkontos auszustellen. Er stellt einige unterschiedliche Funktionalitäten zur Zertifikatsausstellung zur Verfügung: Eine Auflistung der verfügbaren Zertifizierungsstellen, eine Auflistung der verfügbaren Computervorlagen, die Möglichkeit Zertifizierungsanfragen über den Kontext des lokalen Computers zu erstellen und zu übertragen und vieles mehr. Außerdem ermöglicht es der Dienst den Administratoren PFX-Dateien **(**Personal Information Exchange) auf Ihrer Maschine zu installieren. Wenn dieser Dienst angehalten wird, sind Administratoren nicht mehr in der Lage Computerzertifikate auszustellen und PFX-Dateien zu installieren.

DHCP Client

Dieser Dienst verwaltet die Netzwerkkonfiguration, indem er IP-Adressen und Domain Naming Service (DNS) Einträge aktualisiert. Wenn er angehalten wird, erhält der Computer keine dynamischen IP-Adressen mehr. Außerdem werden keine dynamischen DNS-Updates mehr auf dem DNS-Server registriert.

DHCP Server

Dieser Dienst weist IP-Adressen zu und ermöglicht die automatische Konfiguration weiterer Netzwerkeinstellungen, wie zum Beispiel DNS-Server und WINS-Server, von DHCP Clients. DHCP verwendet ein Client/Server Model. Der Netzwerkadministrator richtet einen oder mehrere DHCP-Server ein, der die DHCP-Clients mit TCP/IP-Konfigurationen versorgt.

DHCP ist ein IP-Standard, um die IP-Adressverwaltung im Netzwerk zu vereinfachen. Windows Server 2003 stellt einen DHCP-Server nach dem RFC (Request for Comments) Standard 2131 zur Verfügung. DHCP umfasst unter anderem auch MADCAP (Multicast Address Dynamic Client Assignment Protocol), das für die Mulicast-Adresszuweisung verwendet wird. Wenn registrierte Clients über MADCAP dynamische IP-Adressen anfordern, können sie zum Beispiel Video- oder Audiostreams empfangen. Wenn der Dienst angehalten wird, erhalten die Clients keine IP-Adressen mehr.

Verteiltes Dateisystem (DFS)

Dieser Dienst verwaltet die logischen Laufwerke im Netzwerk. Er wird für die Active Directory SYSVOL- Freigabe benötigt. DFS ist ein verteilter Dienst, der unterschiedliche Freigaben in einen einzelnen logischen Namensraum integriert. Wenn er angehalten wird, sind die Benutzer nicht mehr in der Lage über diesen Namensraum auf Netzwerkfreigaben zuzugreifen. Benutzer müssen dann wieder die exakten Namen aller Freigaben und Server kennen.

Überwachung verteilter Verknüpfungen (Client)

Dieser Dienst ist für die Verwaltung von Verknüpfungen zu NTFS-Dateien zuständig. Er stellt sicher, dass Verknüpfungen und OLE-Links auch nach der Umbenennung oder Verschiebung der Zieldatei noch funktionieren. Wenn Sie in einer NTFS-Partition eine Verknüpfung erstellen, markiert dieser Dienst die Zieldatei mit einer eindeutigen ID. Diese wird zusätzlich in der Verknüpfung gespeichert. So kann in den folgenden Situationen die Quelldatei ermittelt werden:

- Die Zieldatei der Verknüpfung wird umbenannt.
- Die Zieldatei der Verknüpfung wird in einen anderen Ordner auf derselben Partition oder auf eine andere Partition auf demselben Computer verschoben.
- Die Zieldatei der Verknüpfung wird auf einen anderen Computer im Netzwerk verschoben.

  Anmerkung: Außer wenn der Computer einer Domäne angehört, in der dieser Dienst zur Verfügung steht, funktioniert die Überwachung in dieser Situation nicht sehr zuverlässig.

- Der freigegebene Ordner, in der die Zieldatei liegt wird umbenannt.

In einer Windows 2000 oder Windows Server 2003 Domäne, in der dieser Dienst zur Verfügung steht, wird die Zieldatei auch in den folgenden zusätzlichen Situationen noch wieder gefunden:

- Der Computer mit der Zieldatei wird umbenannt.
- Die Partition, auf der die Zieldatei gespeichert ist, wird auf einen anderen Computer derselben Domäne verschoben.

Auf Computern unter Windows XP SP1 muss die Einstellung **DLT_AllowDomainMode** aktiviert sein. Die Zieldatei der Verknüpfung muss in jedem Fall auf einer NTFS-Partition unter Windows 2000, Windows XP oder Windows Server 2003 gespeichert sein. Es darf sich nicht um ein Wechselmedium handeln.

Anmerkung: Der Dienst überwacht die Aktivitäten auf NTFS-Partitionen und speichert diese Informationen in einer Datei mit dem Namen *Tracking.log*. Diese wird in dem versteckten Ordner *System Volume Information* gespeichert. Auf diesen Ordner hat nur das System Zugriff. Der Indexdienst verwendet den Dienst ebenfalls.

Wenn der Dienst angehalten wird, können die Verknüpfungen auf Ihrem Computer nicht aktuell

gehalten werden.

Überwachung verteilter Verknüpfungen (Server)

Dieser Dienst speichert Information so, dass zwischen Partitionen verschobene Dateien nachverfolgt werden können. Er ist standardmäßig deaktiviert. Wenn er aktiviert wird, muss dies auf allen Domänencontrollern der Domäne geschehen. Weitere Informationen finden Sie im Knowledge Base Artikel Q312403 (englischsprachig).

Distributed Transaction Coordinator

Der DTC-Dienst ist für die Koordination von Transaktionen, die über mehrere Computer verteilt sind, verantwortlich. Dies sind zum Beispiel Datenbanken, Nachrichtenwarteschlangen und Dateisysteme. Wenn Transaktionskomponenten über COM+ konfiguriert werden, ist der Dienst notwendig. Wenn er angehalten wird, finden verteilte Transaktionen nicht statt.

DNS-Client

Der Dienst löst DNS-Namen von Computern auf und speichert diese. Er muss auf jedem Computer, der eine DNS-Namensauflösung durchführt, ausgeführt werden. Die DNS-Namensauflösung ist in Active Directory-Domänen zur Lokalisierung von Domänencontrollern zwingend erforderlich. Er wird außerdem zur Lokalisierung von Geräten, welche die DNS-Namensauflösung verwenden, benötigt. Der DNS-Client unter Windows Server 2003 bietet die folgenden Features:

- **Systemweites Cachen:** Resource Records (RR) werden in den lokalen Cache aufgenommen.
- **RFC-konformes negatives Cachen:** Zusätzliche zu den positiven Abfragen cacht der DNS-Client auch die negativen Antworten der DNS-Server. Eine negative Antwort entsteht, wenn für den abgefragten Namen kein RR vorhanden ist. Sie werden allerdings nicht so lange wie die positiven Antworten gecacht - standardmäßig nicht länger als fünf Minuten. Durch das Cachen von negativen Antworten wird die Systemleistung verbessert.
- **Vermeidung von DNS-Servern, die nicht antworten:** Der DNS-Client verwendet eine Serversuchliste. Diese umfasst alle bevorzugten und alternativen DNS-Server, die für die Netzwerkverbindungen des Systems konfiguriert sind. Windows Server 2003 ordnet diese Liste basierend auf den folgenden Kriterien neu:
    - Bevorzugte DNS-Server haben erste Priorität.
    - Wenn kein bevorzugter DNS-Server zur Verfügung steht, werden die alternativen DNS-Server verwendet.
    - Server, die nicht antworten, werden temporär aus der Liste entfernt.

Wenn der Dienst angehalten wird, ist der Computer nicht mehr in der Lage DNS-Namen aufzulösen und Domänencontroller zu finden.

DNS-Server

Dieser Dienst beantwortet Anfragen zur DNS-Namensauflösung und nimmt DNS-Aktualisierungen vor. Ein DNS-Server wird in Active Directory Domänen zur Lokalisierung von Domänencontrollern und zur Lokalisierung von Geräten mit DNS-Namensauflösung zwingend benötigt. Wenn der Dienst angehalten oder deaktiviert ist, finden keine Aktualisierungen mehr statt.

Fehlerberichterstattungsdienst

Dieser Dienst sammelt und speichert Informationen über unerwartete Anwendungsfehler. Er leitet diese dann an Microsoft weiter. Die Produktteams von Microsoft erhalten über ihn Informationen für die Fehlersuche in Treibern und Anwendungen. Sie können bei Betriebssystemfehlern, Fehlern in Windows- Komponenten und Programmfehlern Fehlerberichte an Microsoft senden lassen. Ein Betriebssystemfehler ist aufgetreten, wenn das Betriebssystem mit einem STOPP-Fehlerbildschirm anhält. Auf Programmfehler kann auf zwei Arten reagiert werden: Sofort bei deren Auftreten und beim nächsten Anmelden des Administrators. Windows behandelt Betriebssystemfehler und ungeplantes Herunterfahren anders als Programmfehler. Wenn diese auftreten, schreibt Windows die Fehlerinformationen in eine Protokolldatei. Wenn sich ein Administrator das nächste Mal anmeldet, wird diesem der Fehlerbericht angezeigt.

Wenn sie einen Fehlerbericht über das Internet an Microsoft senden, stehen diese technischen Informationen den Microsoft-Entwicklern für die Entwicklung späterer Programmversionen zur Verfügung. Diese Daten werden ausschließlich für die Qualitätskontrolle, nicht zum Sammeln von Daten über Benutzer oder über Programminstallationen, verwendet.

Sie können die Fehlerberichterstattung auch alternativ über Gruppenrichtlinien konfigurieren und so alle Fehlerberichte intern sammeln. Dann können Sie selbst entscheiden, welche Fehlerberichte an Microsoft weitergeleitet werden sollen. Sie können in der Gruppenrichtlinie einen Pfad zu einem Dateiserver angeben. Die Fehlerberichte werden dann an diesen umgeleitet. Mit dem Fehlerberichterstattungtool können Sie dann einzelne Fehler an Microsoft weiterleiten. Sie können das Tool über die Office XP Resource Kit Webseite unter http://www.microsoft.com/office/ork/xp/default.htm (englischsprachig) herunterladen. Wenn der Dienst angehalten wird, findet keine Fehlerberichterstattung mehr statt.

Ereignisprotokoll

Dieser Dienst ermöglicht das Anzeigen von Ereignisnachrichten, die von Windows-Programmen und -Komponenten ausgelöst wurden. Das Ereignisprotokoll enthält Informationen, die für die Fehlersuche und zur Diagnose von Problemen nützlich sein können. Es speichert Ereignisse, die durch Anwendungen, Dienste und durch das Betriebssystem ausgelöst werden können. Die Protokolle können über die Ereignissprotkoll-API oder über das Snap-In Ereignisanzeige angezeigt werden. Standardmäßig gibt es auf Computern unter Windows Server 2003 die folgenden drei Protokolle:

- **Anwendungsprotokoll:** Enthält die Ereignisse, die von Anwendungen oder Programmen ausgelöst wurden. Zum Beispiel einen Dateifehler eines Datenbankprogramms. Die zu protokollierenden Ereignisse werden vom Entwickler der Anwendung festgelegt.
- **Sicherheitsprotokoll:** Enthält Ereignisse wie gültige und ungültige Anmeldeversuche und Ereignisse, die sich auf den Zugriff auf Ressourcen beziehen. Wenn die Anmeldeüberwachung aktiviert ist, werden deren Ereignisse in diesem Protokoll aufgezeichnet.
- **Systemprotokoll:** Enthält die durch Windows Systemkomponenten ausgelösten Ereignisse. Zum Beispiel Fehler in Treibern oder Systemkomponenten, oder Treiber die beim Systemstart nicht korrekt geladen oder gestartet werden konnten.

Auf einen Domänencontroller unter Windows Server 2003 gibt es zwei zusätzliche Protokolle:

- **Verzeichnisprotokoll:** Enthält die durch den Verzeichnisdienst ausgelösten Ereignisse. Zum Beispiel Verbindungsprobleme zwischen dem Server und dem globalen Katalogserver.
- **Replikaktionsprotokoll:** Enthält Ereignisse, die durch den Dateireplikaktionsdienst ausgelöst wurden. Zum Beispiel Fehler der Dateireplikation zwischen Domänencontrollern.

Auf Computern, die als DNS-Server konfiguriert sind, gibt außerdem folgendes Protokoll:

- **DNS-Protokoll:** Enthält alle Ereignisse, die vom DNS-Server Dienst ausgelöst wurden.

Der Dienst kann nicht angehalten werden. Wenn er deaktiviert ist, werden keine Ereignisse mehr aufgezeichnet. Damit verlieren Sie bei Systemproblemen einen großen Teil Ihrer Diagnosemöglichkeiten.

Fax-Dienst

Dieser Dienst ist ein Telephony-API (TAPI) konformer Dienst, der die Möglichkeit zum Versenden und zum Empfang von Fax-Nachrichten bietet. Benutzer können so aus ihren Anwendungen heraus ein lokales Fax-Gerät oder ein freigegebenen Netzwerkgerät nutzen. Der Dienst bietet die folgenden Features:

- Faxe senden und empfangen.
- Faxaktivitäten überwachen und verfolgen.
- Eingehende Faxe umleiten.
- Verwaltung der Server- und Gerätekonfiguration.
- Gesendete Faxe archivieren.

Wenn der Druckerwarteschlange- oder der Telefonie-Dienst deaktiviert ist, startet der Fax-Dienst nicht. Wenn der Dienst angehalten wird, sind Sie nicht in der Lage, Faxe zu versenden oder zu empfangen.

Dateireplikation

Dieser Dienst ermöglicht das automatische Kopieren von Dateien auf mehrere Server. Eine Funktion des Dateireplikationsdienstes (File Replication Service - FRS) ist die Replikation der Sysvol-Freigabe auf Domänencontrollern. Außerdem kann er für die Dateireplikation über DFS verwendet werden.

Wenn der Dienst angehalten wird, findet keine Dateireplikation mehr statt. Die Daten des Servers werden nicht synchronisiert. In Fall eines Domänencontrollers kann das Anhalten des Dienstes ernsthafte Auswirkungen auf dessen Funktion haben.

Dateiserver für Macintosh

Dieser Dienst ermöglicht es Benutzern von Macintosh Computern auf Dateien auf Computern unter Windows Server 2003 zuzugreifen.

FTP Publishing Service

Dieser Dienst stellt die FTP-Konnektivität und die Verwaltungsmöglichkeit über das Snap-In Microsoft Internet Information Server (IIS) zur Verfügung. Features sind unter anderem: Bandbreitenanpassung, Sicherheitskonten und einer erweiterte Protokollierung. Die neue FTP-Benutzerisolierung gestattet den Benutzern nur den Zugriff auf die Dateien des FTP-Servers.

Hilfe und Support

Dieser Dienst stellt die Möglichkeit zur Verfügung, dass Hilfe- und Supportcenter eines Computers zu verwenden. Er dient zur Kommunikation zwischen der Client-Anwendung und den Hilfe-Daten. Wenn Sie Features des Hilfe- und Supportcenters verwenden, führt dieser Dienst die Datentransaktionen durch. Wenn er auf manuell gesetzt ist, wird er durch einen Zugriff auf das Hilfe- und Supportcenter gestartet. Wenn er deaktiviert ist, erhält der Benutzer beim Zugriff auf das Hilfe- und Supportcenter folgende Fehlermeldung: *Windows kann das Hilfe- und Supportcenter nicht öffnen, da ein Systemdienst nicht ausgeführt wird.* Der Benutzer kann zwar auf einige Hauptpunkte des Hilfe- und Supportcenters zugreifen, die meisten Features stehen allerdings nicht mehr zu Verfügung. Die .HLP- und .CHM-Dateien können jedoch weiterhin angezeigt werden.

HTTP SSL

Dieser Dienst ermöglicht es den IIS SSL-Funktionen zu verwenden. Diese stellen eine sichere Möglichkeit dar, elektronische Transaktionen durchzuführen. Wenn er angehalten wird, können die IIS keine SSL-Funktionen mehr durchführen.

Eingabegerätezugang

Dieser Dienst stellt einen Zugriff über die Standardschnittstellen zur Verfügung. Dies sind zum Beispiel benutzerdefiniert Tasten auf einer Tastatur, Fernbedienungen und andere Multimedia-Geräte. Wenn er angehalten wird, funktionieren unter anderem die zusätzlichen Hotkeys auf USB-Tastaturen nicht mehr.

IAS Jet-Datenbankzugriff

Dieser Dienst ist nur unter den 64-Bit Versionen von Windows Server 2003 verfügbar. Er verwendet das RADIUS-Protokoll, um Dienste zur Authentifizierung, Autorisierung und Kontenverwaltung zur Verfügung zu stellen. IAS kann als RADIUS-Proxy verwendet werden, um RADIUS-Nachrichten zwischen RADIUS-Clients (Zugangsservern) und RADIUS-Servern zu routen.

Eine Infrastruktur zur RADIUS-Authentifizierung und -Autorisierung besteht aus den folgenden Komponenten:

Zugangsclients

Ein Zugangsclient ist ein Gerät, das einen Zugriff auf ein größeres Netzwerk benötigt. Zum Beispiel Einwahl- oder VPN-Clients, drahtlose Clients oder LAN-Clients, die mit einem Switch verbunden sind.

RADIUS-Clients (Zugangsserver)

Ein Zugangsserver ist ein Gerät, das Zugriff auf ein größeres Netzwerk bietet. Ein Zugangsserver, der eine RADIUS-Infrastruktur verwendet, ist auch ein RADIUS-Client. Zugangsserver sind zum Beispiel:

- **Network Access Servers (NAS):** Stellen den Zugang zum Netzwerk einer Organisation oder zum Internet zur Verfügung. Zum Beispiel ein Windows 2000 Computer, der den Routing- und RAS-Dienst ausführt.
- **Wireless Access Points:** Bieten über die Netzwerkschicht Zugriff auf das Netzwerk einer Organisation.
- **Switches:** Bieten über die Netzwerkschicht Zugriff auf das Netzwerk einer Organisation.

RADIUS-Proxies

Ein RADIUS-Proxy ist ein Gerät, das RADIUS-Verbindungsanfragen zwischen RADIUS-Clients, RADIUS-Proxys und RADIUS-Servern weiterleitet oder routet. Er verwendet die in der RADIUS-Nachricht enthaltenen Informationen, zum Beispiel den Benutzernamen oder die aufrufende Station, um die RADIUS-Nachricht zum entsprechenden RADIUS-Server zu routen.

RADIUS-Server

Ein RADIUS-Server ist ein Gerät, das Verbindungsanfragen annimmt und verarbeitet. Basierend auf definierten Regeln und den Informationen der Benutzerdatenbank, führt der RADIUS-Server entweder eine Authentifizierung und Autorisierung durch und schickt eine Access-Accept-Nachricht oder eine Access-Reject-Nachricht. Die Access-Accept-Nachricht enthält dann die für die Verbindung geltenden Verbindungseinschränkungen.

Benutzerkonten-Datenbank

Die Benutzerdatenbank ist eine Liste von Benutzerkonten und deren Eigenschaften. Der RADIUS-Server kann sie verwenden, um die Authentifizierungsinformationen zu prüfen. Die

Konteneigenschaften enthalten außerdem Parameter für die Verbindung. Die Benutzerdatenbank, die IAS verwenden kann sind die lokale SAM, eine Windows NT 4.0 Domäne oder das Active Directory. Mit Active Directory kann IAS eine Authentifizierung und Autorisierung für folgendes durchführen:

- Benutzer- oder Computerkonten aus der Domäne, in der der IAS-Server Mitglied ist.
- Domänen mit bidirektionalen Vertrauensstellungen und vertrauten Gesamtstrukturen, deren Domänencontroller unter Windows Server 2003 ausgeführt werden.

Wenn sich das Benutzerkonto in einer anderen Datenbank als der IAS-Standarddatenbank befindet, können Sie IAS als RADIUS-Proxy konfigurieren. Die Anfragen werden dann an den RADIUS-Server weitergeleitet, der Zugriff auf die entsprechende Datenbank hat.

Es gibt zwei IAS Jet-Datenbanken - Ias.mdb wird für die Konfiguration von IAS verwendet und Dnary.mdb wird von IAS für die Verwendung von herstellerspezifischen RADIUS-Eigenschaften benötigt. Verändern Sie diese Datenbank nicht. Wenn der IAS Jet-Datenbankzugriff-Dienst angehalten wird, ist ein Remotezugriff auf das Netzwerk nicht mehr möglich. Einwahl-, VPN- und Drahtlosverbindungen funktionieren nicht mehr. Wenn der Dienst deaktiviert wird, starten die Dienste Routing und RAS und IAS nicht mehr.

IIS-Verwaltung

Dieser Dienst ermöglicht die Administration von IIS-Komponenten. Das sind zum Beispiel FTP-Anwendungen, Webseiten, Webdienst-Erweiterungen und virtuelle Server für NNTP und SMTP. Wenn er deaktiviert ist, könnten Sie keine Webseiten, FTP-, NNTP- oder SMTP-Dienst verwenden. Unter Windows 2000 wird der Dienst standardmäßig installiert. Unter Windows Server 2003 müssen Sie ihn explizit installieren.

IMAPI CD Brenn COM Dienste

Dieser Dienst verwaltet das Brennen von CDs über die IMAPI COM-Schnittstelle (Image Mastering Applications Programming Interface) und führt das Schreiben auf CD-Rs durch. Die API unterstützt die folgenden Formate: Redbook Audio und Daten-CDs als Joliet und ISO 9660. Die Architektur ermöglicht zukünftige Erweiterungen der unterstützten Formate. Wenn der Dienst angehalten oder deaktiviert wird, sind Sie nicht mehr in der Lage, über die systemeigenen Features CDs zu brennen. Drittanbieteranwendungen sind hiervon nicht betroffen.

Indexdienst

Dieser Dienst indiziert die Inhalte und Eigenschaften von lokalen Dateien und Dateien auf anderen Computern. Er bietet über eine flexible Abfragesprache einen schnellen Zugriff auf Dateien. Über diesen Dienst werden Suchanfragen nach Dokumenten auf dem lokalen Computer, anderen Computern im Netzwerk oder im Internet durchgeführt. Er baut einen Index aller Textinformationen in Dateien und Dokumenten auf. Dieser Index wird er bei jeder Datei, die erstellt, geändert oder gelöscht wird, gepflegt. Die erste Erstellung des Index kann sehr Ressourcenintensiv sein. Normalerweise verwendet der Indexdienst nur die ungenutzte Rechenzeit. Über das Index Snap-In können Sie diese Einstellung ändern. Die MMC ermöglicht auch das Anpassen der Indizierungsmuster. Wenn der Dienst angehalten wird, sind textbasierte Suchanfragen langsamer.

Infrarotüberwachung

Dieser Dienst ermöglicht das Austauschen von Dateien und Bildern über die Infrarotschnittstelle. Er wird nur installiert, wenn während der Installation von Windows Server 2003 eine Infrarotschnittstelle erkannt wird. Er steht unter den Versionen Web, Enterprise und Datacenter Server von Windows Server 2003 nicht zur Verfügung.

Internet Authentifizierungsdienst (IAS)

Dieser Dienst führt eine zentrale Authentifizierung, Autorisierung, Überwachung und Kontenverwaltung für Benutzerverbindungen im LAN, über VPNs oder über RAS durch. IAS implementiert das RADIUS-Protokoll der IETF (Internet Engineering Task Force). Wenn der Dienst deaktiviert oder angehalten ist, werden Authentifizierungsanfragen an einen Sicherungs-IAS-Server weitergeleitet. Wenn es keinen Sicherungsserver gibt, sind die Benutzer nicht in der Lage eine Verbindung mit dem Netzwerk aufzubauen.

Internetverbindungsfirewall (Internet Connection Firewall, ICF)/Gemeinsame Nutzung der Internetverbindung (Internet Connection Sharing, ICS)

Dieser Dienst stellt Netzwerkadressübersetzung (NAT), Adressierung, Namensauflösung und Schutz vor Eindringlingen von außen für alle Computer eine Heim- oder Small-Office-Netzwerkes zur Verfügung. Dies geschieht entweder über ein Einwähl- oder eine Breitbandverbindung. Wenn der Dienst aktiviert ist, wird Ihr Computer zum Internet-Gateway des Netzwerkes. Andere Computer können dann die Internetverbindung, die Freigaben und die Drucker dieses Computers verwenden. Der Dienst hieß unter Windows 2000 Internet Connection Sharing. Wenn er angehalten wird, stehen Netzwerkdienste, wie zum Beispiel die Internetfreigabe und die Namensauflösung nicht mehr zu Verfügung. Die Clients des Netzwerkes können möglicherweise nicht mehr auf das Internet zugreifen. Ihre IP-Adressen könnten ablaufen. Das würde dazu führen, dass die Clients APIPA (Automatic Private IP Addressing) verwenden.

Standortübergreifender Messagingdienst

Dieser Dienst ermöglicht das Austauschen von Nachrichten zwischen Computern an verschiedenen Active Directory Standorten. Er wird zur mailbasierten Replikation mit SMTP über IP verwendet. Die SMTP-Unterstützung ist eine Komponente der IIS. Da die Transportmöglichkeiten für eine Inter-Standortreplikation erweiterbar bleiben sollen, ist jede Transportmöglichkeit über eine separate DLL umgesetzt worden. Diese DLLs werden in den standortübergreifenden Messagingdienst geladen. Dieser wird auf allen Domänencontrollern ausgeführt, die möglicherweise standortübergreifende Replikationen durchführen müssen. Wenn er angehalten wird, wird keine standortübergreifende Replikation durchgeführt. Außerdem stehen anderen Diensten keine standortbezogenen Routinginformationen mehr zu Verfügung.

IP Version 6 Hilfsdienst

Dieser Dienst bietet über ein bestehendes IPv4-Netzwerk eine Internet Protocol Version 6 (IPv6)-Konnektivität. IPv6 ist ein neues Standardprotokollpaket für die Netzwerkschicht des Internets. Über dieses sollen viele der in der aktuellen Version IPv4 bestehenden Probleme behoben werden. Dieser Dienst, oft auch als "6to4" bezeichnet, ermöglicht es Webseiten und Hosts die IPv6 verwenden mit IPv6 über eine IPv4-Infrastruktur zu kommunizieren. 6to4 ist eine Tunneling-Technik, die in RFC 3056 beschrieben wird. 6to4 benötigen keine manuelle Konfiguration und erstellen die 6to4-Adressen automatisch. 6to4 verwendet den globalen Adresspräfix 2002:WWXX:YYZZ::/48, wobei WWXX:YYZZ den hexadezimalen Wert der IPv4-Adresse darstellt (w.x.y.z), die einer Webseite oder einem Host zugewiesen ist. Dieser Teil einer 6to4-Addresse wird auch Next Level Aggregator (NLA) genannt. Der Dienst unterstützt außerdem 6over4, auch bekannt als IPv4 Multicast Tunneling. Diese Tunneling-Technik ist in RFC 2529 beschrieben. 6over4 ermöglicht es IPv6 und IPv4 Knoten mit IPv6 über eine IPv4-Infrastruktur zu kommunizieren. 6over4 verwendet die IPv4-Infrastruktur als multicast-fähige Verknüpfung. Damit 6over4 korrekt funktioniert, muss in der IPv4-Infrastruktur Multicast möglich sein.

Wenn der Dienst angehalten wird, steht IPv6-Konnektivität nur noch zur Verfügung, wenn der Computer mit einem echten IPv6-Netzwerk verbunden ist.

IPSec-Dienste

Dieser Dienst stellt eine Ende-zu-Ende-Sicherheit zwischen Clients und Servern eines TCP/IP-Netzwerkes zur Verfügung, verwaltet die IPSec-Richtlinien, startet den Internet-Schlüsselaustausch (IKE) und koordiniert die Einstellungen der IPSec-Richtlinie mit dem IP-Security Treiber. Er wird über die Befehle NET START und NET STOP konfiguriert. IPSec arbeitet auf der IP-Schicht und ist für andere Betriebssystemdienste und Anwendungen vollständig transparent. Der Dienst ermöglicht eine Paketfilterung. Die Sicherheit kann zwischen sendendem und empfangendem Computer ausgehandelt werden. Über IPSec erreichen sie folgendes:

- Eine Paketfilterung.
- Eine ausgehandelte sichere IP-Kommunikation. Das IKE-Protokoll authentifiziert basierend auf Richtlinieneinstellungen Sender und Empfänger von IP-Paketen gegenseitig. Die Authentifizierung kann über Kerberos, Zertifikate oder einen geheimen Schlüssel (ein Passwort) durchgeführt werden. Schlüssel und Sicherheitszuordnungen werden von IKE automatisch erstellt.
- IPSec stellt die Integrität, Authentizität und Verschlüsselung von geschützten IP-Paketen sicher.
- Sichere Ende-zu-Ende Verbindungen durch IPSec im Transportmodus.
- Sichere IP-Tunnel durch IPSec im Tunnelmodus.

IPSec stellt außerdem sichere L2TP VPN-Verbindungen (Layer Two Tunneling Protocol) zur Verfügung. Wenn der Dienst angehalten wird, wird die Sicherheit zwischen den Clients und Servern des Netzwerkes beeinträchtigt.

Kerberos-Schlüsselverteilungscenter

Dieser Dienst bietet Benutzern die Möglichkeit, sich über das Kerberos5 Authentifizierungsprotokoll am Netzwerk anzumelden. Wie bei anderen Implementierungen des Kerberos-Protokolls auch, ist das Kerberos Schlüsselverteilungscenter (Kerberos Key Distribution - KDC) ein einzelner Prozess, der zwei Dienste zur Verfügung stellt:

Authentifizierungsdienst: Dieser Dienst stellt Ticket Granting Tickets (TGT) für Verbindungen zum Ticket Granting Service der eigenen oder aller vertrauten Domänen aus. Bevor ein Client ein Ticket für einen anderen Computer anfordern kann, muss er beim Autorisierungsdienst seiner Kontodomäne ein TGT anfordern. Der Autorisierungsdienst gibt ein TGT für den Ticket Granting Service der Domäne des Zielcomputers zurück. Das TGT kann so lange wiederverwendet werden, bis es abgelaufen ist. Für den ersten Zugriff auf den Ticket Granting Service einer Domäne ist jedoch immer erst einer Authentifizierung in der Kontodomäne erforderlich.

Ticket Granting Service (TGS): Dieser Dienst stellt Tickets für Verbindungen zu Computern der eigenen Domäne aus. Wenn ein Client auf einen Computer zugreifen will, muss er ein TGT anfordern.

Wenn der Dienst angehalten wird, sind die Benutzer nicht mehr in der Lage sich am Netzwerk anzumelden und auf Ressourcen zuzugreifen.

Lizenzprotokollierung

Dieser Dienst überwacht Clientzugriffslizenzen für Teile des Betriebssystems. Dies schließt IIS, Terminalserver, Datei- und Druckserver und Produkte, die nicht Teil des Betriebssystems sind (zum Beispiel SQL Server und Microsoft Exchange Server), mit ein. Wenn der Dienst angehalten oder deaktiviert wird, wird die Lizenzierung zwar durchgesetzt, jedoch nicht überwacht.

Verwaltung logischer Datenträger

Dieser Dienst erkennt und überwacht neue Festplatten und stellt dem **Verwaltungsdienst für die**

Verwaltung logischer Datenträger Informationen für deren Konfiguration zu Verfügung, indem er auf Plug and Play Ereignisse reagiert. Er verwendet einen Verwaltungsdienst und einen Überwachungsdienst. Der Verwaltungsdienst startet nur, wenn Sie ein Laufwerk, eine Partition oder eine neue Festplatte konfigurieren. Wenn Sie dynamische Datenträger verwenden, sollten Sie den Dienst nicht deaktivierten. Wenn er angehalten wird, kann es zum Beispiel passieren, dass Festplatten nicht erkannt werden.

Verwaltungsdienst für die Verwaltung logischer Datenträger

Dieser Dienst führt administrative Anfragen zur Verwaltung von Festplatten aus und konfiguriert die Festplatten und Partitionen. Er wird nur gestartet, wenn ein logischer Datenträger konfiguriert oder neu erkannt wird, oder wenn das Snap-In Datenträgerverwaltung oder das Tool Diskpart.exe verwendet werden. Aktionen, die einen Start verursachen sind zum Beispiel die Konvertierung einer Festplatte von basis zu dynamisch, die Wiederherstellung von fehlertoleranten Volumes, die Formatierung oder das Verschieben der Auslagerungsdatei. Der Dienst wird nur für die Dauer des Vorgangs ausgeführt. Danach wird er automatisch wieder angehalten. Wenn der Dienst deaktiviert ist, wird bei Verwendung des Snap-Ins Datenträgerverwaltung die folgende Fehlermeldung angezeigt: *Es kann keine Verbindung mit dem Dienst Verwaltung logischer Datenträger aufgebaut werden.*

Nachrichtenwarteschlange

Bei diesem Systemdienst handelt es sich um eine Nachrichteninfrastruktur und ein Entwicklungswerkzeug für die Erstellung von verteilten Nachrichtenanwendungen. Solche Anwendungen können über heterogene Netzwerke hinweg kommunizieren und Nachrichten zwischen Computern verschicken, die zeitweise keine Verbindung miteinander aufbauen können. Über Nachrichtenwarteschlangen werden die Nachrichtenzustellung, das effiziente Routen, die Sicherheit und die prioritätsbasierte Verarbeitung sichergestellt. Der Dienst stellt für die gesamte Programmierungsfunktionalität eine Microsoft® Win32 und eine COM API zur Verfügung. Wenn der Dienst deaktiviert wird, sind andere Dienste, unter anderem einige COM+ Komponenten, einige Funktionalitäten von WMI und der **MSMQ Triggers**-Dienst davon betroffen.

Message Queuing Down Level Clients

Dieser Systemdienst stellt Message Queuing Clients, Windows 9x, Windows NT 4.0 und Windows 2000 auf Domänencontroller einen Active Directory Zugriff zur Verfügung. Wenn er im Workgroup-Modus installiert wird, wird nicht auf Active Directory zugegriffen.

Message Queuing Triggers

Dieser Dienst bietet eine regelbasierte Überwachung von in Nachrichtenwarteschlangen eintreffenden Nachrichten. Wenn eine Regel zutrifft, wird eine COM-Komponente oder ein eigenständiges ausführbares Programm zur Verarbeitung der Nachricht gestartet. Der Dienst wird als integraler Bestandteil des Dienstes Message Queuing installiert. Dieser ist eine optionale Windows-Komponente und steht in allen Windows-Versionen außer Windows XP Home Edition zur Verfügung.

Nachrichtendienst

Dieser Systemdienst verwendet oder empfängt Nachrichten von Benutzern, Computern, Administratoren oder dem Warndienst. Er hat nichts mit dem Windows Messenger, einem kostenlosen Instant-Messaging- Dienst des MSN, zu tun. Wenn er deaktiviert wird, können auf dem Computer keine Nachrichten mehr empfangen oder versendet werden. Die Befehle NET SEND und NET NAME stehen nicht mehr zu Verfügung.

Microsoft POP3-Dienst

Dieser Dienst ist für die Übertragung und den Empfang von E-Mails verantwortlich. Administratoren können ihn verwenden, um E-Mail-Konten auf Mailservern zu speichern und zu verwalten. Wenn Sie diesen Dienst auf einem Mailserver installieren, können die Benutzer sich mit diesem Server verbinden und über einen E-Mail Client, der das POP3-Protokoll unterstützt, E-Mails abrufen. Für eine vollständige E-Mail-Funktionalität ist außerdem der SMTP-Dienst notwendig. Dieser ermöglicht das Versenden von E-Mails. Wenn der POP3-Dienst angehalten wird, ist kein E-Mail-Transfer mehr möglich.

Microsoft Software-Schattenkopieanbieter

Dieser Systemdienst verwaltet die softwarebasierten Schattenkopien des Volumenschattenkopie-Anbieters. Eine Schattenkopie ermöglicht es Ihnen eine Momentaufnahme eines Laufwerkes zu erstellen. Es gibt zwei generelle Arten von Schattenkopien:

- **Hardware:** Eine Hardware Schattenkopie ist ein Spiegelsatz aus zwei oder mehr Platten.
- **Software:** Eine Software Schattenkopie kopiert alle geänderten Sektoren eines Volumens in einen speziellen Bereich.

Schattenkopien können bei drei klassischen Aufgaben der Datensicherung eingesetzt werden:

- Wenn Dateien gesichert werden müssen, die exklusiv geöffnet sind.
- Wenn das System während einer Sicherung weiter aktiv sein soll.
- Wenn dieselben Kommunikationskanäle verwendet werden sollen, die für den Informationstransfer zwischen Anwendungen und Sicherungstools verwendet werden.

Die Plattform für Schattenkopien setzt sich aus den folgenden Komponenten zusammen:

- Ein Satz von APIs für die Anwendungssynchronisation.
- Ein Schattenkopie Gerätetreiber, der Volumenschattenkopien für alle lokalen Volumes bietet.
- Support für die Sync- und Provider-APIs.

Wenn der Dienst angehalten wird, können die softwarebasierten Volumenschattenkopien nicht mehr verwaltet werden.

MSSQL$UDDI

Der MSSQL$UDDI-Dienst (Universal Description Discovery and Integration - UDDI) ist ein Industriestandard für die Veröffentlichung und Lokalisierung von Informationen über Webdienste. Windows Server 2003 stellt UDDI-Dienste zur Verfügung. Die Kernkomponente dieses Features ist eine SQL Server Datenbankengine.

MSSQLServerADHelper

Dieser Dienst gibt dem SQL-Serverdienst und dem SQL Server-Analysedienst die Möglichkeit, Informationen im Active Directory zu veröffentlichen, wenn diese beiden Dienste nicht unter dem Konto Lokales System ausgeführt werden.

.NET Framework-Unterstützungsdienst

Dieser Dienst benachrichtigt einen Client, wenn ein bestimmter Prozess den Client Runtime Dienst initialisiert. Er stellt eine Laufzeitumgebung zur Verfügung. Diese wird Common Language Runtime

genannt, und ist für die Ausführung von Programmcode verantwortlich. Sie stellt Dienste für eine einfachere Entwicklung zur Verfügung. Die CLR ermöglicht es Ihnen, Komponenten und Anwendungen zu entwickeln, deren Objekte über Programmiersprachen hinweg kommunizieren können.

Anmeldedienst

Dieser Dienst verwaltet einen sichereren Kanal für die Authentifizierung zwischen einem Computer und dem Domänencontroller. Er übergibt über diesen Kanal die Anmeldeinformationen an den Domänencontroller und erhält die Security Identifier (SIDs) und Benutzerrechte des Benutzers zurück. Dieser Vorgang wird Pass-Trough-Authentifizierung genannt. Wenn ein Computer Mitglied einer Domäne ist, startet der Dienst automatisch. Unter Windows Server 2003 und Windows 2000 veröffentlicht der Anmeldedienst Diensteinträge im DNS, und verwendet den DNS um Namen und IP-Adressen der Domänencontroller aufzulösen. Er implementiert außerdem die Replikation über RPC (Remote Procedure Call) zur Synchronisation mit Windows NT 4.0 PDCs (Primary Domain Controllers) und BDCs (Backup Domain Controllers). Wenn der Dienst angehalten wird, ist der Computer nicht mehr in der Lage Benutzer und Dienste zu authentifizieren. Domänencontroller können keine DNS-Einträge mehr registrieren.

NetMeeting Remotedesktop Freigabe

Dieser Dienst gibt autorisierten Benutzern die Möglichkeit, mit Microsoft NetMeeting® über das Netzwerk auf den Computer zuzugreifen. Er kann über NetMeeting aktiviert und über NetMeeting oder den Infobereich der Taskleiste deaktiviert werden.

Netzwerkverbindungen

Dieser Dienst verwaltet den Ordner Netzwerkverbindungen, über den Netzwerk- und Wählverbindungen angezeigt werden können. Er ist für die Netzwerkkonfiguration auf Clientseite verantwortlich und zeigt den Status in der Taskleiste an. Außerdem können Sie über ihn auf die Konfigurationseinstellungen zugreifen. Der Dienst wird automatisch gestartet, wenn eine Netzwerkverbindung aufgerufen wird. Wenn er angehalten wird, ist eine clientseitige Konfiguration von LAN-, Einwähl- oder VPN-Verbindungen nicht mehr möglich. Wenn der Dienst deaktiviert ist, könnte folgendes passieren:

- Verbindungen werden in den Netzwerkeigenschaften nicht mehr angezeigt.
- Komponenten, die den Dienste Netzwerkverbindungen verwenden, zum Beispiel Gruppenrichtlinien, funktionieren nicht mehr korrekt.
- Ereignisse die Mediaverbindungen betreffen, werden nicht mehr ausgelöst.
- Die Internetverbindungsfreigabe funktioniert nicht mehr korrekt.
- Es ist nicht mehr möglich eingehende Verbindungen, drahtlose Verbindungen oder das Heimnetzwerk zu konfigurieren.
- Es werden keine Netzwerkverbindungen erstellt.
- Jeder Dienst, der von diesem Dienst abhängig ist, wird nicht gestartet.

Netzwerk DDE Dienst

Dieser Dienst stellt den Netzwerktransport und die Sicherheit für Dynamic Data Exchange (DDE) für Programme zur Verfügung. Sie können Netzwerk DDE Freigaben per Programm oder über die Verwendung von Ddeshare.exe erstellen. Normalerweise startet der Benutzer, der eine Freigabe erstellt, einen Serverprozess, um die eingehenden Client- und Anwendungsanfragen zu handhaben. Sobald sie verbunden sind, können diese Prozesse alle möglichen Daten über eine sichere

Netzwerkverbindung austauschen. Dieser Dienst ist standardmäßig deaktiviert. Er wird nur gestartet, wenn er durch eine Anwendung die Netzwerk-DDE verwendet, zum Beispiel Clipbrd.exe oder Ddeshare.exe, aufgerufen wird. Wenn der Dienst deaktiviert ist, starten die Anwendungen, die ihn verwenden, nicht mehr korrekt.

Netzwerk DDE Serverdienst

Dieser Dienst verwaltet die DDE-Netzwerkfreigaben. Er wird ausschließlich vom DDE-Netzwerkdienst verwendet. Sie können DDE-Netzwerkfreigaben mit Ddeshare.exe erstellen. Der Dienst verwaltet eine Datenbank mit DDE-Freigaben. Für jede Verbindungsanfrage von oder zu einer Anwendung fragt der Dienst die Datenbank ab und prüft die Sicherheitseinstellungen.

NLA (Network Location Awareness)

Dieser Dienst sammelt und speichert Informationen zur Netzwerkkonfiguration, wie zum Beispiel geänderte IP-Adressen und Domänennamen. Wenn sein Startyp auf manuell steht, wird er automatisch gestartet.

Network News Transport Protocol (NNTP)

Dieser Dienst ermöglicht es Windows Server 2003 als Newsserver zu agieren. Der Newsserver von Windows Server 2003 unterstützt keine Replikation zwischen mehreren Newsservern. Diese kann nur über die Newsserver-Version von Exchange 2000 durchgeführt werden.

NT LM Sicherheitsdienst

Dieser Dienst stellt für RPC-Programme, die Transporte nicht über Named-Pipes durchführen, Sicherheit zur Verfügung. Er ermöglicht es Benutzern, sich über das NTLM-Authentifizierungsprotokoll am Netzwerk anzumelden. Über dieses Protokoll können Clients authentifiziert werden, die nicht in der Lage sind, das Kerberos5-Protokoll zu verwenden. Das Windows NT Challenge/Response NTLM-Authentifizierungsprotokoll wird in Netzwerken verwendet, in denen Systeme unter Windows NT-Versionen vor Windows 2000 und eigenständige Systeme eingesetzt werden. NTLM steht für Windows NT LAN Manager. Es handelt sich um eine weiterentwickelte Version des schwächeren LAN Manager (LM)-Protokolls. Seit Windows 2000 steht mit dem Microsoft Kerberos Sicherheitspaket eine bessere Sicherheit zur Verfügung als mit NTLM. Obwohl in Windows 2000 Netzwerken Kerberos eingesetzt wird, steht NTLM noch immer zur Verfügung. Es wird in Netzwerken eingesetzt, in denen Clients mit älteren Betriebssystemen als Windows 2000 vorhanden sind. Die Anmeldeauthentifizierung auf eigenständigen Systemen wird ebenfalls über NTLM durchgeführt.

NTLM-Anmeldeinformationen basieren auf den Daten, die währen der interaktiven Anmeldung gesammelt wurden. Dies sind Domänenname, Benutzername und ein Einweg-Hash des Benutzerpasswortes. NTLM verwendet ein verschlüsseltes Challenge/Response-Protokoll für die Authentifizierung der Benutzer. Das Passwort wird nicht über das Netzwerk gesendet. Stattdessen muss das System, das eine Authentifizierung anfordert, beweisen, dass es Zugriff auf die abgesicherten NTLM-Anmeldeinformationen hat.

An einer interaktiven NTLM-Anmeldung über ein Netzwerk sind typischerweise zwei Systeme beteiligt: Ein Clientsystem, auf dem der Benutzer eine Authentifizierung anfordert und ein Domänencontroller, auf dem das Benutzerpasswort hinterlegt ist. An einer nicht-interaktiven Anmeldung, die zum Beispiel beim Zugriff eines bereits angemeldeten Benutzers auf eine Serverressource notwendig wird, sind normalerweise drei Systeme beteiligt: Ein Client, ein Server, und ein Domänencontroller, der die Authentifizierung anstelle des Servers durchführt. Wenn der Dienst angehalten oder deaktiviert wird, sind Sie nicht mehr in der Lage, sich an Clients über das NTLM-Protokoll anzumelden und auf Netzwerkressourcen zuzugreifen. Der Microsoft Operations Manager (MOM) ist von diesem Dienst abhängig.

Leistungsprotokolle und Warnungen

Dieser Dienst sammelt Leistungsdaten des lokalen Computers oder eines Netzwerkcomputers. Diese Sammlung basiert auf der vorkonfigurierten Planung. Er schreibt die gesammelten Daten in ein Protokoll oder löst einen Alarm aus. Er wird nur ausgeführt, wenn mindestens eine Datensammlung geplant wurde.

Plug & Play

Dieser Dienst ermöglicht es einem Computer mit geringer oder keiner Unterstützung durch den Benutzer Hardwareänderungen zu erkennen und anzupassen. Plug and Play ermöglicht das Hinzufügen und Entfernen von Geräten ohne tiefgreifendes Wissen über Computerhardware und ohne eine manuelle Konfiguration von Betriebssystem oder Hardware durchführen zu müssen. Der Dienst kann über das Snap-In Dienste nicht beendet oder gestartet werden, da dies schwerwiegende Auswirkungen auf die Stabilität des Betriebssystems hätte. Wenn er über das Tool MSCONIFIG angehalten wird, werden im Gerätemanager keine Geräte mehr angezeigt.

Seriennummer der tragbaren Medien

Dieser Dienst sammelt die Seriennummern aller tragbaren Musik-Abspielgeräte, die mit dem Computer verbunden sind. Über diese können Inhalte sicher auf solche Geräte kopiert werden. Ohne Seriennummern können Sie Inhalte nicht einem speziellen Gerät zuweisen. Daher kann es sein, dass geschützte Inhalte nicht auf ein bestimmtes Gerät transferiert werden können.

Druckserver für Macintosh

Dieser Dienst ermöglicht es Macintosh-Clients Druckaufträge an eine Druckwarteschlange eines Computers unter Windows Server 2003 Enterprise Server zu senden. Er wird von Windows Server 2003 außerdem für die Kommunikation über das AppleTalk-Protokoll verwendet.

Druckerwarteschlange

Dieser Dienst verwaltet alle lokalen und Netzwerkdruckwarteschlangen. Er kontrolliert alle Druckaufträge und kommuniziert mit Drucktreibern und Eingabe/Ausgabe-Komponenten. Wenn der Dienst angehalten wird, schlagen das Drucken und das Versenden von Faxen auf dem Computer fehl, da er nicht automatisch neu gestartet wird.

Geschützter Speicher

Dieser Dienst schützt Speicherbereiche mit sensiblen Informationen, wie zum Beispiel private Schlüssel und verhindert den Zugriff durch nicht autorisierte Dienste, Prozesse oder Benutzer. Die Speicherbereiche werden über eine Hash-basierte Authentifizierung und den SHA1-Algorithmus (Secure Hash Algorithm 1) geschützt. Der Dienst wurde durch die Data Protection API (DPAPI) ersetzt, die nun für den Schutz von Speicherbereichen verwendet wird. Wenn der Dienst angehalten wird, ist kein Zugriff auf die privaten Schlüssel mehr möglich, der Zertifikatsserver funktioniert nicht, S/MIME (Secure Multipurpose Internet Mail Extensions) und SSL stehen nicht zur Verfügung, und die Smartcardanmeldung schlägt fehl.

Verwaltung für automatische RAS-Verbindung

Dieser Dienst erkennt erfolglose Versuche einer Verbindung mit einem Remotenetzwerk oder einem anderen Computer. Er stellt dann alternative Methoden für eine Verbindung zu Verfügung. Wenn ein Programm nicht in der Lage ist, auf einen DNS- oder NetBIOS-Namen oder eine Adresse zuzugreifen,

bietet dieser Dienst an, eine Wähl- oder VPN-Verbindung aufzubauen. Er pflegt eine lokale Datenbank der zuletzt verwendeten Verbindungen. Schlägt ein Zugriff auf die Freigabe eines Remotecomputers fehl, sucht der Dienst in dieser Datenbank nach der als letztes zum Zugriff auf die Freigabe verwendeten Verbindung. Diese wird dem Benutzer dann vorgeschlagen. Wenn der Dienst angehalten ist, müssen Verbindungen zu Remotecomputern manuell aufgebaut werden.

RAS-Verbindungsverwaltung

Dieser Dienst verwaltet Wähl- und VPN-Verbindungen, die vom Computer zum Internet oder zu anderen Netzwerken aufgebaut werden. Wenn Sie eine Verbindung über den Ordner Netzwerkverbindungen starten, dann wird diese von der RAS-Verbindungsverwaltung aufgebaut und ausgehandelt. Wenn keine Verbindungsanfragen mehr ausstehen, wird der Dienst beendet. Wenn der Dienst angehalten ist, ist der Computer nicht mehr in der Lage, Einwähl- oder VPN-Verbindungen aufzubauen oder auf eingehende Verbindungen zu antworten. Außerdem wird im Ordner Netzwerkverbindungen nichts mehr angezeigt.

Remoteverwaltungsdienst

Dieser Dienst ist beim Serverstart für die Ausführung der folgenden Aufgaben zur Fernadministration verantwortlich:

- Den Startzähler des Servers erhöhen.
- Ein selbstsigniertes Zertifikat erstellen.
- Eine Warnmeldung erstellen, wenn auf dem Server Datum und Uhrzeit nicht konfiguriert sind.
- Eine Warnmeldung erstellen, wenn die E-Mail-Benachrichtigung nicht konfiguriert wurde.

Der Dienst führt die entsprechenden Aufgaben aus, wenn diese vom Remoteverwaltungsdienst über eine COM-Schnittstelle angefordert werden. Er wird unter dem lokalen Systemkonto ausgeführt, und Anfragen an die COM-Schnittstelle werden angenommen, wenn sie vom Administratorkonto oder dem lokalen Systemkonto stammen. Wenn der Dienst auf manuell konfiguriert ist, wird er auf Anfrage des Remoteverwaltungsdienstes automatisch gestartet.

Sitzungs-Manager für Remotedesktophilfe

Dieser Dienst kontrolliert und verwaltet die Remote-Hifefunktion der Hilfe- und Support-Center-Anwendung (helpctr.exe). Wenn er angehalten wird, steht die Remoteunterstützung nicht mehr zur Verfügung.

Remoteinstallation

Dieser Dienst ermöglicht die Installation von Windows 2000, Windows XP und Windows Server 2003 auf PXE-fähigen Computern. Der Boot Information Negotiation Layer (BINL)-Dienst, die primäre Komponenten des Remote Installation Services (RIS), antwortet auf Anfragen von PXE-Clients, überprüft den Client über Active Directory und übergibt die Clientinformationen an den Server. Er wird zusammen mit der RIS-Komponente installiert.

Mit RIS können Sie, unter anderem, folgendes Umsetzen:

- Betriebssystemabbilder für den Abruf durch Benutzer zur Verfügung stellen. Sie können RIS verwenden, um automatisierte Installationsabbilder der folgenden Betriebssysteme zu erstellen: Windows Server 2003, Windows XP und Windows 2000. Wenn ein Benutzer einen Clientcomputer startet, kann der RIS-Server über das Netzwerk ein Betriebssystem installieren. Auch dann, wenn auf dem Clientcomputer noch gar kein Betriebssystem installiert ist. Es wird

keine CD benötigt. Der Client muss allerdings PXE-fähig sein. Das bedeutet, dass er über den Netzwerkadapter booten können muss.

- Betriebssystemabbilder, inklusive spezifischer Einstellungen und Anwendungen, zur Verfügung stellen. Zum Beispiel ein Abbild, das dem Standarddesktop des Unternehmens entspricht. Bestimmten Benutzergruppen können Sie Abbilder zur Verfügung stellen, die Sie speziell für diese Benutzer erstellt haben.

Remoteprozeduraufruf (RPC)

Dieser Dienst ist ein Mechanismus zur sicheren Inter-Prozess Kommunikation. Er ermöglicht es, Daten zwischen verschiedenen Prozessen auszutauschen und abzurufen. Diese verschiedenen Prozesse können auf dem lokalen Computer ausgeführt werden, im LAN oder im Internet verteilt sein. Der Dienst führt eine RCP-Endpunktzuordung durch und ist ein COM Service Control Manager (SCM). Viele Dienste sind für einen erfolgreichen Start vom RPC-Dienst abhängig. Diese sind zum Beispiel: BITS, COM+ Ereignissystem, COM+ Ereignissystem, Zertifikatsdienst, Kryptografiedienste, DHCP Server, Überwachung verteilter Verknüpfungen (Client), Überwachung verteilter Verknüpfungen (Server), Distributed Transaction Coordinator, DNS Server, Fehlerberichterstattungsdienst, Ereignisprotokoll, Fax Service, Dateireplikation, Hilfe und Support, Eingabegerätezugang, IIS-Verwaltung, Indexdienst, IAS, IPSec-Dienste, Kerberos-Schlüsselverteilungscenter, Verwaltung logischer Datenträger, Verwaltungsdienst für die Verwaltung logischer Datenträger, Nachrichtendienst, Microsoft Software Schattenkopieanbieter, Netzwerkverbindungen, Remoteregistrierung, Remote Storage Server, Anbieter des Richtlinienergebnissatzes, Routing und RAS, Sicherheitskontenverwaltung, Shellhardwareerkennung, Taskplaner, Telefonie, Telnet, Terminaldienste, Terminaldienstelizensierung, Terminaldienste-Sitzungsverzeichnis, Upload Manager, Volumeschattenkopie, Windows Audio, Windows-Bilderfassung (WIA) , Windows Installer, Windows Internet Name Service (WINS), Drahtloskonfiguration, WMI-Leistungsadapter, WWW-Publishing.

Der RPC-Dienst kann nicht angehalten oder deaktiviert werden. Dies würde dazu führen, dass das Betriebssystem nicht geladen werden kann.

RPC-Locator

Dieser Dienst ermöglicht es RPC-Clients, die RpcNs* APIs zur Lokalisierung von RPC-Servern zu verwenden, und verwaltet die RPC-Namensdienst Datenbank. Er ist standardmäßig deaktiviert, und wird seit Windows 95 nur noch von sehr wenigen Anwendungen verwendet. Weitere Informationen finden Sie im MSDN unter http://www.microsoft.com/windows/reskits/webresources (englischsprachig). Wenn der Dienst angehalten oder deaktiviert wird, sind RPC-Clients, die seine API verwenden, nicht mehr in der Lage Server zu finden.

Remoteregistrierung

Dieser Dienst ermöglicht es Benutzern die Registrierung des Computers über das Netzwerk zu bearbeiten – vorausgesetzt diese Benutzer haben die passenden Berechtigungen. Normalerweise können nur die Administratoren und die Sicherungsoperatoren von extern auf die Registrierung zugreifen. Der Dienst wird vom Microsoft Baseline Security Analyzer (MBSA) benötigt. Der MSBA ist ein Werkzeug, über das Sie auf den Servern ihrer Organisation die installierten Patches prüfen können. Wenn der Dienst angehalten wird, ist eine Bearbeitung der Registrierung nur noch lokal am Computer möglich. Die Deaktivierung dieses Dienstes beeinflusst den lokalen Zugriff auf die Registrierung nicht.

Remoteserver-Manager

Dieser Dienst stellt die folgenden Funktionalitäten zur Verfügung:

- Speichern der Remoteadministrations-Warnmeldungen.

- Eine Schnittstelle für das Einstellen, Löschen und Anzeigen von Warnmeldungen.
- Eine Schnittstelle zur Durchführung von Administrativen Aufgaben.

Der Dienst arbeitet als WMI-Anbieter. Er führt die entsprechende Aufgabe aus, wenn diese vom Remoteverwaltungsdienst über eine COM-Schnittstelle angefordert wird. Der Dienst wird unter dem lokalen Systemkonto ausgeführt, und Anfragen an die COM-Schnittstelle werden angenommen, wenn sie vom Administratorkonten oder dem lokalen Systemkonto stammen. Wenn der Dienst angehalten ist, wird er beim nächsten Zugriff auf die Remoteadministration wieder gestartet.

Remote Server Monitor

Dieser Dienst bietet eine Überwachung von kritischen Systemressourcen. Er verwaltet möglicherweise vorhandene Überwachungshardware.

Remote Storage Notification

Dieser Dienst benachrichtigt Sie, wenn Sie versuchen, Dateien zu lesen oder zu schreiben, die nur über ein sekundäres Speichermedium verfügbar ist.

Remote Storage Server

Dieser Dienst speichert nicht regelmäßig verwendete Dateien auf sekundären Speichermedien. Er ermöglicht es dem Dienst Remote Storage Notification Sie zu informieren, wenn Sie auf eine Offline-Datei zugreifen.

Wechselmedien

Dieser Dienst verwaltet und katalogisiert Wechselmedien und automatisiert die Kontrolle über die entsprechenden Geräte. Dieser Katalog umfasst Bänder und CDs. Wenn der Computer über automatische Geräte zur Verwaltung von Wechselmedien, zum Beispiel einen Tapeloader oder einen CD-Wechsler, verfügt, automatisiert der Dienst außerdem die Bereitstellung dieser Medien.

Anbieter des Richtlinienergebnissatzes

Dieser Dienst ermöglicht es Ihnen, auf einen Windows Server 2003 Domänencontroller und auf die WMI-Datenbank des lokalen Computers zuzugreifen. Er erstellt den Richtlinienergebnissatz für Gruppenrichtlinien.

Routing und RAS

Dieser Dienst bietet LAN-LAN, LAN-WAN, VPN und NAT-Routingdienst. Zusätzlich stellt er Wähl- und VPN-Verbindungen zu Verfügung. Mit ihm kann Ihr Server als RAS-Server, VPN-Server, Gateway oder Router arbeiten. Als Router unterstützt der Dienst die Protokolle Open Shortest Path First (OSPF) und Routing Information Protocol (RIP). Wenn er angehalten wird, ist der Computer nicht in der Lage, eingehende RAS-, VPN- oder Einwählverbindungen zu verarbeiten.

SAP Agent

Dieser Dienst veröffentlicht in einem IPX-Netzwerk Netzwerkdienste über das IPX Service Advertising Protocol (SAP). Einige Features, wie zum Beispiel der **SAP Agent**, sind von diesem Dienst abhängig. Für die Verwendung des Dienstes ist die Installation des NWLINK-Protokolls nötig.

Sekundäre Anmeldung

Dieser Dienst ermöglicht es Benutzern Prozesse unter dem Kontext eines anderen Sicherheitsprinzipals zu erstellen. Administrationen, die als eingeschränkter Benutzer angemeldet sind, können über diesen Dienst zum Beispiel Anwendungen als Administrator ausführen. Eine Komponente des Dienstes ist das Programm RunAs.exe. Mit dem Befehl RunAs können Sie, während Sie als Benutzer angemeldet sind, Programme (*.exe), gespeicherte MMC-Konsolen (*.msc), Verknüpfungen und Systemsteuerungsoptionen als Administrator ausführen.

Sicherheitskontenverwaltung

Dieser Dienst, auch **Security Accounts Manager** (SAM) genannt, ist ein geschütztes Subsystem, das die Informationen zu Benutzerkonten und Gruppen verwaltet.

Unter Windows 2000 und Windows Server 2003 werden lokale Sicherheitskonten in der Registrierung und Domänenkonten in Active Directory gespeichert. Der Start dieses Dienstes signalisiert anderen Diensten, dass er nun in der Lage ist, Anfragen zu verarbeiten. Er kann nicht angehalten werden. Wenn Sie ihn deaktivieren, verhindert das, dass andere Dienste gestartet werden. Deaktivieren Sie ihn also auf keinen Fall.

Server

Dieser Dienst stellt RPC-Unterstützung und Datei-, Drucker und Named-Pipe-Freigaben zur Verfügung. Bei der Kommunikation über Named-Pipes wird Speicher für die Ausgaben eines Prozesse reserviert. Diese Ausgaben werden dann als Eingabe für einen weiteren Prozess verwendet. Der verarbeitende Prozess muss nicht auf dem gleichen Computer ausgeführt werden. Wenn der Dienst angehalten wird, sind Sie nicht mehr in der Lage Freigaben zu erstellen, und RPC-Anfragen werden nicht mehr beantwortet.

Shell-Hardwareerkennung

Dieser Dienst benachrichtigt Sie bei AutoPlay-Hardwareereignissen. AutoPlay ist ein Feature, das Inhalte wie Bilder, Musik oder Videos auf Wechselmedien erkennt. Es startet dann automatisch die dazugehörige Anwendung. So wird die Verwendung externer Geräte, zum Beispiel MP3-Player, vereinfacht. Die folgenden Geräte werden von AutoPlay unterstützt:

- Wechseldatenträger
- Flashmedien
- PC-Karten
- Externe USB-Laufwerke

Die Unterstützten Medientypen sind:

- Bilder (.jpg, .bmp, .gif, .tif)
- Musikdateien (.mp3, .wma)
- Videos (.mpg, .asf)

Wenn der Dienst angehalten wird, steht die AutoPlay-Funktionalität nicht mehr zur Verfügung.

SMTP

Dieser Dienst wird zur Übertragung und Weiterleitung von E-Mails verwendet. Windows-Domänencontroller verwenden ihn für die standortübergreifende E-Mail-basierte Replikation. Die

CDO-Komponente (Collaboration Data Objekts) von Windows Server 2003 verwendet SMTP zur E-Mail-Übertragung.

Grundlegende TCP/IP-Dienste

Dieser Dienst implementiert die folgenden Protokolle:

- **Echo**, Port 7, RFC 862
- **Discard**, Port 9, RFC 863
- **Character Generator**, Port 19, RFC 864
- **Daytime**, Port 13, RFC 867
- **Quote of the Day**, Port 17, RFC 865

Wenn Sie ihn aktivierten, sind alle fünf Protokolle auf allen Netzwerkadaptern aktiviert. Es gibt keine Möglichkeit nur einzelne Protokolle zu aktivieren oder dies auf einzelne Netzwerkadapter zu beschränken. Das Anhalten dieses Dienstes hat keine Auswirkungen auf den Rest des Betriebssystems. Installieren Sie ihn nicht, wenn Sie den entsprechenden Dienst nicht unbedingt benötigen.

Single Instance Storage Groveler (SIS)

Dieser Dienst ist ein integraler Bestandteil von RIS. SIS verringert den auf dem RIS-Laufwerk erforderlichen Speicherplatz. SIS sucht auf dem Laufwerk nach doppelten Dateien. Wenn solche Dateien gefunden werden, wird die Originaldatei verschoben und an Ihrer Stelle verbleibt nur eine Verknüpfung. Der SIS-Dienst kann nur mit Dateien arbeiten, die auf einer NTFS-Partition gespeichert sind.

Wenn der Dienst angehalten wird, werden keine neuen Verknüpfungen mehr erstellt. Die vorhandenen Verknüpfungen können allerdings weiter verwendet werden.

Smartcard

Dieser Dienst verwaltet den Zugriff auf Smartcards im Smartkartenleser. Das Smartcard-Subsystem basiert auf den Standards des Personal Computer/Smart Card (PC/SC)-Konsortiums, und es setzt sich aus den folgenden Komponenten zusammen:

- Ressourcenmanager**:** Diese Komponente verwaltet den Zugriff auf Lesegeräte und Smartcards. Sie ist für die folgenden Funktionen zuständig:
    - Ressourcen identifizieren
    - Ressourcen anwendungsübergreifend zur Verfügung stellen
    - Zugriff auf die Dienste der jeweiligen Karte zur Verfügung stellen

Der Ressourcenmanager stellt den Anwendungen über die Win32API eine Auswahl der Karten und Lesegerät zur Verfügung.

SNMP

Dieser Dienst ist notwendig, damit eingehende SNMP-Anfragen (Simple Network Management Protocol) vom Computer verarbeitet werden können. Der **SNMP-Dienst** enthält Agenten, die die Aktivitäten der Netzwerkgeräte überwachen. **SNMP** ist ein Verfahren für die Verwaltung von Netzwerkhosts, wie zum Beispiel Arbeitsstationen, Server, Router, Bridges und Hubs, von einer zentralen Stelle aus. SMTP führt diese Verwaltungsdienste über eine verteilte Architektur von

Verwaltungssystemen und Agenten durch. Sie können SNMP für folgendes verwenden:

- **Konfiguration von Remotegeräten:** Von dem Verwaltungssystem können Konfigurationsdaten an jedes Netzwerkgerät geschickt werden.
- **Netzwerkleistung überwachen:** Sie können die Netzwerkleistung überwachen und Informationen über den Erfolg von Datenübertragungen verfolgen.
- **Netzwerkfehler und unberechtigten Zugriff erkennen:** Sie können Alarmauslöser für Netzwerkgeräte definieren. Wenn ein Alarm ausgelöst wird, sendet das Gerät eine Nachricht an das Verwaltungssystem. Typische Alarme treten zum Beispiel bei Herunterfahren und Neustarten von Geräten auf.
- **Netzwerknutzung überwachen:** Sie können sowohl die Gesamtnutzung, als auch die Verwendung durch einzelne Benutzer oder Gruppen überwachen.

Der SNMP-Dienst umfasst einen SNMP-Agenten der die Verwaltung von Computern unter folgenden Betriebssystemen ermöglicht:

- Windows XP Home Edition
- Windows XP Professional
- Windows 2000 Professional
- Windows 2000 Server
- Windows Server 2003

Die folgenden Dienste können über den SNMP-Agenten verwaltet werden:

- WINS unter Windows XP, Windows Server 2003 und Windows 2000
- DHCP unter Windows XP, Windows Server 2003 und Windows 2000
- Internet Information Services unter Windows XP, Windows Server 2003 und Windows 2000
- LAN Manager

Wenn der Dienst angehalten wird, antwortet der Computer nicht mehr auf SNMP-Anfragen.

SNMP Trap-Dienst

Dieser Dienst empfängt Trap-Nachrichten die durch lokale oder remote SNMP-Agenten generiert wurden. Er leitet diese dann an die SNMP-Verwaltungsprogramme weiter. Wenn der SNMP-Dienst als Agent konfiguriert ist, erzeugt er beim Auftreten eines Ereignisses eine Trap-Nachricht. Diese schickt er dann an ein Trap-Ziel. Ein solches Ereignis könnte zum Beispiel das Eintreffen einer Anfrage eines unautorisierten SNMP-Systems sein. Trap-Ziele bestehen aus dem Computernamen oder der IP-Adresse des Verwaltungssystems. Auf diese muss eine SNMP-Verwaltungssoftware ausgeführt werden. Wenn der Dienst angehalten wird, können die SNMP-basierten Programme Ihres Computers keine SNMP-Trap Nachrichten mehr empfangen.

Hilfsprogramm für spezielle Verwaltungskonsole (SAC)

Sie können, wenn ein System unter Windows Server 2003 mit einer Stopp-Meldung beendet wird, über diesen Dienst Remoteverwaltungsaufgaben durchführen. Die Hauptfunktionen dieses Dienstes sind:

- Umleiten der Fehlermeldung der Stopp-Meldung.
- Das System neu starten.
- Informationen zur Identifikation des Computers erlangen

Der Dienst ist eine unabhängige Notfall-Kommandozeilenumgebung, die über Windows Server 2003 zur Verfügung gestellt wird.

SQLAgent$* (* UDDI oder WebDB)

Dieser Dienst wird zu Aufgabenplanung und Überwachung verwendet. Er verschiebt Informationen zwischen SQL-Servern und wird für die Sicherung und Replikation verwendet. Wenn der Dienst angehalten wird, findet keine SQL-Replikation mehr statt.

System Ereignisbenachrichtigung

Dieser Dienst überwacht und verfolgt Systemereignisse und benachrichtigt die Abonnenten des COM+ Ereignissystems. Wenn er angehalten wird, kommt es zu folgenden Problemen:

- Die Win32 APIs IsNetworkAlive() und IsDestinationReachable() funktionieren nicht mehr. Diese APIs werden oft von mobilen Anwendungen auf Notebooks genutzt.
- Die ISens* Schnittstellen funktionieren nicht mehr.
- SyncMgr (mobsync.exe) funktioniert nicht mehr korrekt.
- Das COM+ Ereignissystem schlägt fehl.

Taskplaner

Dieser Dienst ermöglicht es Ihnen automatisierte Tasks zu planen und zu konfigurieren. Er überwacht die Kriterien, die Sie ausgewählt haben. Wenn diese zutreffen, führt er die geplanten Aufgaben aus. Sie können die folgenden Aktionen über den Taskplaner durchführen:

- Task zur Ausführung zu einer bestimmten Uhrzeit oder bei einem bestimmten Ereignis planen.
- Den Zeitplan für einen Task ändern
- Anpassen, wie die Tasks ausgeführt werden
- Einen geplanten Task anhalten

Sie können den Taskplaner über das *Dienste* Snap-In starten. Sie können über die graphische Benutzerschnittstelle, die Task Scheduler API oder über das Werkzeug SchTasks.exe zugreifen. Wenn der Dienst angehalten wird, werden die geplanten Tasks nicht ausgeführt. Softwareupdates über den Systems Management Server schlagen fehl.

TCP/IP NetBIOS Hilfsdienst

Dieser Dienst ermöglicht NetBIOS über TCP/IP (NetBT) und die NetBIOS-Namensauflösung. Wenn er angehalten wird, sind NetBT, Redirector (RDR), Server (SRV) und Netlogon Clients nicht mehr in der Lage, Dateien und Drucker freizugeben und Anmeldungen durchzuführen. Domänenbasierte Gruppenrichtlinien funktionieren zum Beispiel nicht mehr.

TCP/IP-Druckserver

Dieser Dienst ermöglicht TCP/IP-basiertes Drucken über das Line Printer Daemon Protocol.

Telefonie

Dieser Dienst bietet TAPI-Unterstützung für Programme, die Telephoniegeräte steuern. Auch IP-

basierte Sprachverbindungen werden von ihm gesteuert. Wenn er angehalten oder deaktiviert wird, können alle Dienste, die von diesem abhängig sind, zum Beispiel die Modemunterstützung, nicht mehr starten. Er kann nicht angehalten werden, wenn ein von ihm abhängiger Dienst, wie zum Beispiel RAS, aktiv ist. Wenn er angehalten ist, wird der Dienst bei einem erneuten Aufruf der TAPI-Schnittstelle neu gestartet.

Telnet

Dieser Dienst stellt eine ASCII Terminalsitzung für Telnet-Clients zur Verfügung. Telnet-Server bieten zwei verschiedene Authentifizierungen und unterstützten vier Terminaltypen: ANSI (American National Standards Institute), VT-100, VT-52 und VTNT. Telnet ermöglicht es, Benutzer sich am System anzumelden und Konsolenprogramme über eine Eingabeaufforderung auszuführen. Ein Computer, der den Telnet-Dienst ausführt, kann mehrere TCP/IP Telnet-Clients bedienen. Der Starttyp des veralteten Telnet-Dienstes ist standardmäßig auf deaktiviert gesetzt.

Terminaldienste

Dieser Dienst bietet eine Umgebung mit mehrfachen Sitzungen. Diese ermöglicht es Clients auf virtuelle Windows Desktopsitzungen auf dem Server zuzugreifen. Über den Terminaldienst können sich mehrere Benutzer interaktiv am Computer anmelden. Als Standard ist er im Remoteadministrationsmodus installiert. Um ihn im Anwendungsmodus zu installieren, verwenden Sie die Option Software in der Systemsteuerung. Um die Remotebenutzung des Computers zu verhindern, sollten Sie die Kontrollkästchen **Remoteunterstützung zulassen** und **Remotedesktop zulassen** auf der Registerkarte **Remote** in den Systemeigenschaften deaktivieren.

Terminaldienste Lizenzierung

Dieser Dienst installiert einen Lizenzserver und stellt registrierten Clients bei einer Verbindung zum Terminalserver Lizenzen zur Verfügung. Wenn er deaktiviert wird, können den Clients von Terminalserver keine Lizenzen zur Verfügung gestellt werden.

Terminaldienste Sitzungsverzeichnis

Dieser Dienst ermöglicht es Terminalserver-Clustern zur Lastverteilung die Verbindungsanforderung des Benutzers an den Server umzuleiten, auf dem er bereits eine Sitzung ausführt. Wenn er angehalten wird, wird der Benutzer an den ersten verfügbaren Terminalserver umgeleitet – egal ob er auf einem anderen Server des Clusters bereits eine Sitzung geöffnet hat.

Designs

Dieser Dienst verwaltet die Designs der graphischen Benutzerschnittstelle von Windows XP. Ein Desktop Design ist ein vorgefertigter Satz von Symbolen, Schriften, Farben, Tönen und anderen Windows-Elementen. Wenn der Dienst angehalten wird, wird das alte Windows-Design verwendet.

Trivial FTP Daemon

Trivial FTP (TFTP) benötigt keinen Benutzernamen oder ein Passwort und ist integraler Bestandteil von RIS. Der Dienst implementiert die Unterstützung für das durch die folgenden RFCs definierte TFTP-Protokoll:

- RFC 1350 - TFTP
- RFC 2347 - Option extension

- RFC 2348 - Block size option
- RFC 2349 - Timeout interval and transfer size options

Ein RIS-Server verwendet TFTPD für das Herunterladen der Initialdateien, die für den Start des Remoteinstallationsprozesses erforderlich sind. Wenn der Dienst angehalten wird, sind Clientcomputer nicht mehr in der Lage, den RIS-Server zu verwenden.

Unterbrechungsfreie Stromversorgung

Dieser Dienst verwaltet die mit dem Computer über eine serielle Schnittstelle verbundenen unterbrechungsfreien Stromversorgungen.

Upload Manager

Dieser Dienst verwaltet die synchronen und asynchronen Dateiübertragungen zwischen den Clients und den Servern des Netzwerkes. Es werden anonyme Treiberdaten von der Maschine des Kunden zum Server von Microsoft übertragen. Anhand dieser Daten werden dann die für das System benötigten Treiber gesucht. Die übertragenen Daten umfassen die Hardware-Identifikationsnummer des Gerätes und eine ID für das verwendete Betriebssystem. Es kann kein Rückschluss auf einen Benutzer, einen Computer, ein Unternehmen, eine IP-Adresse oder eine andere Quelle geschlossen werden. Sie werden verwendet, um festzustellen, für welche Geräte Treiber fehlen. Microsoft versucht dann diese zusammen mit dem Hersteller zur Verfügung zu stellen.

Dienst für virtuelle Datenträger

Dieser Dienst stellt eine hersteller- und technologienabhängige Schnittstelle für die Verwaltung von logischen Volumes (Software) und logischen Einheiten (Hardware) zur Verfügung.

Volumenschattenkopie

Dieser Dienst implementiert und verwaltet Volumenschattenkopien. Über ihn werden die Volumensnapshots verwaltet. Er stellt fest, von welchen Volumes eine Sicherung durchgeführt werden muss. Diese werden dann an den Shadow Copy Coordinator übergeben, und es wird eine Schattenkopie erstellt. Schattenkopien sind Volumes, die dem Zustand des Originalvolumens zum Zeitpunkt der Sicherung entsprechen.

WebClient

Dieser Dienst erlaubt es Win32-Anwendungen auf Dokumente im Internet zuzugreifen. Er erweitert die Netzwerkkapazität von Windows, indem normale Win32-Anwendungen über WebDAV Dateien auf Internet Dateiservern zugreifen können. Das WebDAV-Protokoll ist ein Dateizugriffsprotokoll, das in XML beschrieben ist. Es wird über das HTTP-Protokoll verwendet und nutzt damit die bestehende Internet-Infrastruktur. Wenn der Dienst angehalten wird, kann der Web-Veröffentlichungsassistent nicht mehr verwendet werden.

Web Element Manager

Dieser Dienst ist für die folgenden Elemente der Administrationswebseite unter Port 8098 verantwortlich:

- Registerkarten der Administrationswebseite
- Remoteadministrationstasks

- Inhaltesverzeichnis
- Hilfe
- Remoteadministrationswarnungen

Ein Administrator kann einen Server über die URL https://servername:8098 remote verwalten. Wenn eine Verbindung zu dieser Webseite aufgebaut wird, werden die oben aufgelisteten Informationen von der ASP-Seite über diesen Dienst abgefragt. Der Dienst wird unter dem lokalen Systemkonto ausgeführt und beantwortet nur Anfragen des Administratorkontos oder des lokalen Systemkontos. Wenn er angehalten wird oder auf manuell gesetzt ist, wird er bei der nächsten Anfrage über die Webschnittstelle gestartet.

Windows Audio

Dieser Dienst stellt Audioausgaben zur Verfügung. Er verwaltet Plug and Play-Audiogeräte, wie zum Beispiel Soundkarten. Sobald der Dienst einmal gestartet wurde, kann er nicht angehalten werden.

Windows-Bilderfassung (WIA)

Dieser Dienst ermöglicht die Übernahme von Bildern von Scannern und Kameras. Windows Server 2003 unterstützt Geräte, welche die Windows Driver Model (WDM)-Architektur verwenden.

Windows Installer

Dieser Dienst verwaltet die Installation und die Entfernung von Anwendungen über definierte Setup-Regeln. Diese Regeln definieren die Installation und Konfiguration der installierten Anwendung. Sie können über den Dienst bestehende Anwendungen ändern, reparieren oder entfernen. Die Windows Installer-Technologie setzt sich aus dem Dienst und dem .msi-Dateiformat zusammen. Wenn der Dienst auf den Starttyp manuell konfiguriert ist, wird er durch eine Anwendung, die ihn verwenden will, gestartet. Wenn der Dienst angehalten ist, schlägt die Installation, Entfernung, Reparatur und Änderung solcher Anwendungen fehl. Einige Anwendungen verwenden den Dienst während sie ausgeführt werden. Solche Anwendungen können in diesem Fall nicht ausgeführt werden.

Windows Internet Name Service (WINS)

Dieser Dienst ermöglicht die NetBIOS-Namensauflösung. Solange nicht alle Domänencontroller auf Active Directory aktualisiert wurden und alle Computer im Netzwerk Windows 2000 oder höher ausführen, sind WINS-Server erforderlich. Wenn der Dienst angehalten wird, passiert folgendes:

- Windows NT4 Domänen und Domänencontroller können nicht mehr gefunden werden.
- Windows NT4 Clients können keine Windows 2000 oder Windows Server 2003 Active Directory Domänen und Domänencontroller mehr finden.
- Die NetBIOS-Namensauflösung schlägt fehl, es sei denn, das gesuchte Gerät befindet sich im selben Subnetz, und die NetBIOS-Namensauflösung wird über Broadcasts durchgeführt.

Windows Verwaltungsinstrumentarium

Dieser Dienst bietet eine allgemeine Schnittstelle und ein Objektmodell, um auf Verwaltungsinformationen zu Betriebssystem, Geräten, Anwendungen und Diensten zuzugreifen. WMI ist eine Infrastruktur für die Erstellung von Verwaltungsanwendung. Die WMI-Infrastruktur ist eine Betriebssystemkomponente, die Informationen über verwaltete Objekte speichert und zur Verfügung stellt. Sie besteht aus zwei Komponenten: Dem Dienst und dem WMI-Repository. Der Dienst arbeitet als Vermittler zwischen Anbietern, Verwaltungsanwendungen und dem WMI-Repository. Er schreibt

Informationen von einem Anbieter in das WMI-Repository. Außerdem fragt er das Repository ab. Das WMI-Repository speichert die Informationen, die es von verschiedenen Anbietern bekommt. Den Zugriff stellt WMI über einige Schnittstellen, unter anderem eine COM API, Script und Kommandozeilenbefehle, zur Verfügung. WMI ist kompatibel mit SNMP. Wenn der Dienst angehalten wird, funktionieren die meisten Windows-basierten Programme nicht mehr korrekt.

Treibererweiterungen für Windows-Verwaltungsinstrumentarium

Dieser Dienst überwacht alle Treiber und Ereignisanbieter die WMI- oder Ereignis-Informationen veröffentlichen.

Windows Media Dienste

Dieser Dienst stellt Steaming-Media-Dienste über IP-basierte Netzwerke zur Verfügung. Er ersetzt die vier Einzeldienste der Windows Media Dienste Version 4.0 und 4.1:

- Windows Media Überwachungsdienst
- Windows Media Programmdienst
- Windows Media Senderdienste
- Windows Media Unicast Dienst

Die Kernkomponenten des Dienstes wurden über COM entwickelt. Er unterstützt deutlich mehr Protokolle als vorher – zum Beispiel das Real Time Streaming Protocol (RTSP), das Microsoft Media Server (MMS) Protocol und HTTP. Die Windows Mediendienste-Plattform setzt sich aus den folgenden Industriestandards zusammen: WMI, SNMP, XML, Synchronized Multimedia Integration Language (SMIL) 2.0, Document Object Model (DOM) und Moving Picture Experts Group (MPEG) 1 und 2.

Windows System Resource Manager

Dieser Dienst soll den Kunden bei der Bereitstellung von Anwendungen helfen. Über ihn ist die richtlinienbasierte Verwaltung des Speicherverbrauchs und der CPU-Auslastung von Prozessen möglich. Die CPU-Verwaltung wird über das Zuweisen einer prozentualen Bandbreite durchgeführt. Die Speicherverwaltung umfasst das Setzen von Einschränkungen und das Zuweisen von maximalen Speichergrenzen zu Prozessen.

Windows Zeitgeber

Dieser Dienst pflegt die Datums- und Zeitsynchronisation. Er verwendet das Network Time Protocol (NTP) zur Synchronisation der Computeruhren. Auf Computern, die nicht einer Domäne angehören, können Sie eine externe Zeitquelle konfigurieren. Die Deaktivierung dieses Dienstes kann zu zwei möglichen Szenarios führen:

- Wenn der Dienst auf einer Arbeitsstation angehalten oder deaktiviert wird, kann die Arbeitsstation die eigene Uhrzeit nicht mehr mit anderen Quellen synchronisieren.
- Wenn der Dienst auf einem Domänencontroller angehalten oder deaktiviert wird, tritt derselbe Effekt wie oben auf. Außerdem sind die Domänenmitglieder ebenfalls nicht mehr in der Lage ihre Uhrzeit mit dem Domänencontroller zu synchronisieren. Die kann sich auf die Zeitsynchronisation des gesamten Unternehmens auswirken.

WinHTTP Web Proxy Auto Discovery Dienst

Dieser Dienst implementiert das Web Proxy Auto Discovery (WPAD)-Protokoll für die HTTP-Dienste. WPAD ist ein Protokoll, dass es HTTP-Clients ermöglicht, eine automatische Proxy-Konfiguration zu beziehen.

Drahtloskonfiguration

Dieser Dienst ermöglicht die automatische Konfiguration von IEEE 802.11-Drahtlosadaptern. In Zusammenarbeit mit Herstellern von 802.11 Netzwerkarten (NIC) hat Microsoft die Konfiguration dieser NIC automatisiert. Diese suchen nach verfügbaren Netzwerken und geben diese an Windows .NET weiter. Der Dienst kümmert sich dann um die Konfiguration der NIC.

WMI Leistungsadapter

Dieser Dienst stellt Leistungsbibliothek-Informationen der WMI-HiPerf-Anbieter zur Verfügung. Er wird standardmäßig nicht ausgeführt und steht auf dem Starttyp manuell. Er wird erst gestartet, wenn ein Client, zum Beispiel Sysmon, ihn zur Abfrage von Leistungsdaten verwendet.

Arbeitsstation

Dieser Dienst erstellt und pflegt Client-Netzwerkverbindungen. Wenn er angehalten wird, sind Sie nicht mehr in der Lage Netzwerkverbindungen mit Remoteservern über Named-Pipes aufzubauen. Dies verhindert den Zugriff auf Dateien und Drucker auf anderen Servern, beeinflusst die TCP/HTTP-Konnektivität jedoch nicht.

WWW-Publishing

Dieser Dienst stellt Web-Konnektivität und die Administration von Webseiten über das IIS-Snap-In zu Verfügung. Er ist vom IIS-Verwaltungsdienst und dem TCP/IP-Support des Kernels abhängig. Wenn er angehalten wird, ist Windows Server 2003 nicht in der Lage auf irgendeine Form von Webanfragen zu antworten.

8

Richtlinien für Softwareeinschränkungen

Richtlinien für Softwareeinschränkungen sind ein neues Feature von Microsoft® Windows® XP und Microsoft Windows Server 2003. Sie ermöglichen eine richtliniengesteuerte Spezifizierung der Programme die ausgeführt werden dürfen und der Programme, die nicht ausgeführt werden dürfen. Sie helfen Organisationen dabei, sich gegen bösartigen Programmcode zu schützen. Sie bieten eine weitere Verteidigungsschicht gegen Viren, Trojanische Pferde und anderen Arten von bösartigem Programmcode.

Sicherheitslücken

Durch die steigende Verwendung von Netzwerken und dem Internet bei der täglichen Arbeit ist das Risiko von Beschädigungen durch bösartigen Programmcode so groß wie noch nie. E-Mails können viele Arten von solchem bösartigen Programmcode enthalten. Dies kann von ausführbaren Windows-Programmen (.exe) über Makros in Textverarbeitungsdokumenten (.doc) bis zu Scripts (.vbs) reichen. Viren und Würmer versuchen oft die Benutzer durch die unterschiedlichsten Tricks dazu zu bewegen sie zu aktivieren. Durch die riesige Zahl von Variationen und Formen, in denen diese auftauchen, kann es den Benutzern sehr schwer fallen festzustellen, was sicher ist und was nicht. Bösartiger Programmcode kann die unterschiedlichsten Schäden anrichten: Inhalte der Festplatten beschädigen, Netzwerke mit DoS-Angriffen überziehen, vertrauliche Informationen in das Internet senden oder die Sicherheit eines Computers kompromittieren.

Gegenmaßnahmen

Erstellen Sie ein fehlerfreies Design für die Softwareeinschränkungen der Endbenutzer-Computer Ihrer Umgebung. Testen Sie dies vor einer Bereitstellung in Ihrer Produktionsumgebung sorgfältig in einer Testumgebung.

Mögliche Auswirkungen

Eine fehlerhafte Implementierung von Softwareeinschränkungen führt dazu, dass notwendige Anwendungen nicht mehr ausgeführt und bösartige Anwendungen gestartet werden können.

Anmerkung: Obwohl Softwareeinschränkungen für die Erweiterung der Sicherheit eines Computers ein wichtiges Werkzeug darstellen, sind sie kein Ersatz für andere Sicherheitsmaßnahmen – wie zum Beispiel Virenscannern, Firewalls und restriktive Zugriffskontrolllisten.

9

Administrative Vorlagen von Windows XP, Office XP und Windows Server 2003

Der Abschnitt administrative Vorlagen der Gruppenrichtlinie umfasst registrierungsbasierte Einstellung, die das Verhalten und das Erscheinungsbild der Computer Ihrer Umgebung bestimmen. Sie wirken sich außerdem auf das Verhalten von Betriebssystemkomponenten und Anwendungen aus. Es gibt bereits eine große Menge solcher Einstellung. Sie können durch das Importieren von .adm-Dateien weitere hinzufügen.

Dieses Kapitel beschreibt die unter dem Knoten *Computerkonfiguration* und dem Knoten *Benutzerkonfiguration* vorhandenen administrativen Vorlagen.

Es werden nur die Einstellung unter Microsoft® Windows® XP, Microsoft Office XP und Microsoft Windows Server 2003 besprochen, die für die Absicherung von Computern relevant sind. Die nicht besprochenen Einstellungen beziehen sich unter anderem auf Microsoft NetMeeting®, Anwendungskompatibilität, Taskplaner, Windows Installer, Windows Messenger und den Windows Media® Player.

Internet Explorer Einstellung

Der Microsoft Internet Explorer ist der in Windows XP und Windows Server 2003 enthaltene Webbrowser. Sie können viele seiner Features über die Gruppenrichtlinien verwalten. Sie finden die entsprechenden Einstellungen unter:
Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Internet Explorer

Automatische Installation von Internet Explorer-Komponenten deaktivieren

Die Aktivierung dieser Einstellung verhindert, dass der Internet Explorer Komponenten herunterlädt, wenn der Benutzer Webseiten aufruft, für die diese erforderlich wären. Wenn die Einstellung deaktiviert oder nicht konfiguriert ist, wird der Benutzer jedes Mal zur Installation der Komponenten aufgefordert. Über diese Richtlinie kann der Administrator kontrollieren, welche Komponenten vom Benutzer installiert werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Böswillige Webseitenbetreiber können Komponenten installieren, die schädlichen Programmcode ausführen. Dies könnte zur ungewollten Verbreitung von Daten, zum Verlust von Daten oder zur Instabilität des Systems führen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Der Internet Explorer ist nicht mehr in der Lage, die für Webseiten benötigten Komponenten automatisch herunterzuladen.

Periodische Überprüfungen auf Softwareaktualisierungen von Internet Explorer deaktivieren

Wenn die Einstellung aktiviert ist, wird verhindert, dass der Internet Explorer nach neuen Versionen des Browsers sucht und den Benutzer darüber informiert. Wenn sie deaktiviert oder nicht konfiguriert ist, sucht der Internet Explorer alle **30 Tage** nach neuen Versionen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Obwohl Microsoft alle Patches und Servicepacks vor deren Veröffentlichung ausführlich testet, möchten manche Organisationen möglicherweise eine genauere Kontrolle über die auf ihren Systemen installierten Updates behalten. Wenn die Einstellung aktiviert ist, werden keine Updates für den Internet Explorer heruntergeladen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Der Internet Explorer ist nicht mehr in der Lage, Hotfixes und Servicepacks automatisch herunterzuladen. Daher muss hierfür vom Administrator ein anderes Verfahren implementiert werden.

Anzeigen des Begrüßungsbildschirms deaktivieren

Wenn dieser Einstellung aktiviert ist, wird der Begrüßungsbildschirm – er zeigt Programmname, Lizenz und Copyright-Informationen an - beim Start des Browsers nicht mehr angezeigt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

In einigen Organisationen ist es möglicherweise nicht gewollt, dass den Benutzern die Lizenz und die Version des Internet Explorers bekannt sind.

Gegenmaßnahmen

Setzten Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Der Internet Explorer startet schneller, wenn er keinen Begrüßungsbildschirm anzeigt.

Deaktivieren von Software-Update Shell-Benachrichtigungen beim Programmstart

Diese Einstellung definiert, ob Programme, die den Microsoft Software Distribution Channel verwenden, den Benutzer bei der Installation neuer Komponenten benachrichtigen. Der Software Distribution Channel ist ein dynamisches Softwareupdate über die Open Software Distribution (OSD)-Technologie. Wenn die Einstellung aktiviert ist, werden die Benutzer nicht benachrichtigt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Organisationen, die OSD-Werkzeuge und -Technologien verwenden, möchten möglicherweise, dass die Benutzer bei einer Installation von Patches und Servicepacks auf ihren Systemen nicht benachrichtigt werden. Diese könnten versuchen den Installationsprozess abzubrechen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**

Mögliche Auswirkungen

Benutzer werden bei Updates über OSD-Technologien nicht benachrichtigt.

Proxy-Einstellung pro Computer vornehmen (anstelle von pro Benutzer)

Wenn diese Einstellung aktiviert ist, können die Benutzer keine eigenen Proxy-Einstellungen mehr vornehmen. Sie müssen die Einstellungen verwenden, die für alle Benutzer dieses Computers gelten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn die Einstellung deaktiviert oder nicht konfiguriert ist, können die Benutzer ihre eigenen Proxy-Einstellungen verwenden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Alle Benutzer werden dazu gezwungen, die für den Computer definierten Proxy-Einstellungen zu verwenden.

Sicherheitszonen: Benutzer können Sites nicht hinzufügen oder entfernen

Wenn dieser Einstellung aktiviert ist, ist das Hinzufügen oder Entfernen von Webseiten zu Sicherheitszonen nicht mehr möglich.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Aktivieren Sie alternativ die Einstellung **Sicherheitsseite deaktivieren**, unter *Benutzerkonfiguration\Administrative Vorlagen\Windows Komponenten\Internet Explorer\Internetoptionen*. Sie entfernt die gesamte Registerkarte Sicherheit.

Sicherheitslücken

Wenn die Einstellung nicht konfiguriert ist, ist es den Benutzern möglich die Zoneneinstellungen zu verändern. Sie könnten so auf gefährliche Webseiten zugreifen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Diese Richtlinie verhindert, dass Benutzer die Einstellungen der Sicherheitszonen verändern, die der Administrator vorgenommen hat. Dies kann nur noch der Administrator.

Sicherheitszonen: Benutzer können Einstellung nicht ändern

Die Aktivierung dieser Einstellung bewirkt, dass der Schalter **Stufe anpassen** und der Schieberegler **Sicherheitslevel dieser Zone** auf der Registerkarte **Sicherheit** der **Internetoptionen** nicht mehr zu Verfügung stehen. Wenn die Einstellung deaktiviert oder nicht konfiguriert ist, kann der Benutzer die Sicherheitsoptionen ändern.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Aktivieren Sie alternativ die Einstellung **Sicherheitsseite deaktivieren**, unter *Benutzerkonfiguration\Administrative Vorlagen\Windows Komponenten\Internet Explorer\Internetoptionen*. Sie entfernt die gesamte Registerkarte Sicherheit.

Sicherheitslücken

Wenn die Einstellung nicht konfiguriert ist, ist es den Benutzern möglich die Zoneneinstellungen zu verändern. Sie könnten so auf gefährliche Webseiten zugreifen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Diese Richtlinie verhindert, dass Benutzer die Einstellungen der Sicherheitszonen verändern, die der Administrator vorgenommen hat. Dies kann nur noch der Administrator.

Sicherheitszonen: Die Einstellung für Sicherheitszonen statisch festlegen

Wenn die Einstellung aktiviert ist, werden die Einstellungen, die ein Benutzer vornimmt für alle Benutzer des Computers verwendet. Wenn sie deaktiviert oder nicht konfiguriert ist, verwenden alle Benutzer ihre eigenen Einstellungen für die Sicherheitszonen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn die Einstellung nicht konfiguriert ist, ist es den Benutzern möglich die Zoneneinstellungen zu verändern. Sie könnten so auf gefährliche Webseiten zugreifen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Diese Richtlinie verhindert, dass Benutzer die Einstellungen der Sicherheitszonen verändern.

Terminalserver-Richtlinien konfigurieren

Die Terminaldienste-Komponente von Windows Server 2003 baut auf der soliden Grundlage des Anwendungsserver-Modus der Windows 2000 Terminaldienste auf. Sie stellt nun auch die neuen Möglichkeiten der Windows XP Terminaldienste zur Verfügung. Die Terminaldienste von Windows Server 2003 können die Softwareverteilung eines Unternehmens über eine Vielzahl von Szenarios verbessern. Wenn ein Benutzer eine Anwendung auf einem Terminalserver startet, wir diese auf dem Terminalserver ausgeführt. Nur die Informationen im Bezug auf Tastatur, Maus und Anzeige werden über das Netzwerk übertragen. Jeder Benutzer hat seine eigene Sitzung. Diese wird vom Serverbetriebssystem verwaltet und ist von allen anderen Sitzungen vollständig unabhängig. Sie können die Richtlinieneinstellungen für Terminalserver über den folgenden Pfad konfigurieren: *Computerkonfiguration\Administrative Vorlagen\Windows Komponenten\Terminaldienste*

Abmelden von Administratoren in Konsolensitzung verweigern

Dieser Einstellung definiert, ob es einem Administrator gestattet ist, eine Verbindung zur Konsole eines Servers aufzubauen und damit den momentan an der Konsole angemeldeten Administrator abzumelden. Die Konsolensitzung wird auch Sitzung 0 genannt. Ein Konsolenzugriff kann über den Schalter /console im Feld Computername einer Remotedesktopverbindung, oder über die Eingabeaufforderung durchgeführt werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Wenn diese Einstellung **aktiviert** ist, wird verhindert, dass ein am System angemeldeter Administrator abgemeldet wird und so möglicherweise Daten verloren gehen. Bei den Einstellungen deaktiviert und nicht konfiguriert ist dies möglich.

Sicherheitslücken

Ein Angreifer, der es geschafft hat eine Terminalserver-Sitzung aufzubauen und administrative Privilegien zu erlangen, könnte es dem legalen Administrator sehr schwer machen, die Kontrolle über den Computer über die Sitzung 0 zurückzuerlangen. Wenn ein Angreifer einen solchen Zugriff auf einen Computer erlangt hat, hat dieser allerdings den Computer bereits vollständig übernommen. Daher ist der Wert eventueller Gegenmaßnahmen ehr gering.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Ein Administrator ist nicht in der Lage, andere Administratoren von der Sitzung 0 Konsole abzumelden.

Anpassen der Berechtigungen durch lokale Administratoren nicht zulassen

Diese Einstellung definiert, ob ein Administrator die Sicherheitsberichtigungen im Terminaldienste-Konfigurationstool ändern kann. So können Sie verhindern, dass die Sicherheitsbeschreibungen der Benutzergruppen auf der Registerkarte Berechtigungen geändert werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Die Standardmethode zur Verwaltung des Benutzerzugriffs ist das Hinzufügen der Benutzer zur Gruppe **Remotedesktop-Benutzer**.

Sicherheitslücken

Ein Angreifer, der administrativen Zugriff auf einen Server, der die Terminaldienste ausführt, erlangt hat, kann die Berechtigung ändern und so die Benutzer daran hindern eine Verbindung zum Server aufzubauen. Dies stellt einen DoS-Zustand dar. Wenn ein Angreifer einen solchen Zugriff auf einen Computer erlangt hat, hat dieser allerdings den Computer bereits vollständig übernommen. Daher ist der Wert eventueller Gegenmaßnahmen ehr gering.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Die Sicherheitsbeschreibungen können über die Registerkarte Berechtigungen nicht geändert werden.

Regeln für Remoteüberwachung von Terminaldienste-Benutzersitzungen festlegen

Diese Einstellung legt die Remoteüberwachung fest, die in einer Terminalsitzung gestattet ist. Eine Remoteüberwachung kann mit oder ohne Erlaubnis des Benutzers durchgeführt werden. Über diese Einstellung können Sie zwei unterschiedliche Varianten der Remoteüberwachung konfigurieren: **Sitzung anzeigen** erlaubt die Remoteüberwachung einer Sitzung. **Vollzugriff** erlaubt mit der Sitzung zu interagieren. Wenn die Einstellung aktiviert ist, ist es den Administratoren möglich, in die Terminalsitzung eines Benutzers einzugreifen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Keine Remoteüberwachung erlaubt**
  - **Vollzugriff mit Erlaubnis des Benutzers**
  - **Vollzugriff ohne Erlaubnis des Benutzers**
  - **Sitzung anzeigen mit Erlaubnis des Benutzers**
  - **Sitzung anzeigen ohne Erlaubnis des Benutzers**
- **Deaktiviert**

- **Nicht konfiguriert**

Anmerkung: Diese Einstellung gibt es unter *Computerkonfiguration* und unter *Benutzerkonfiguration*. Wenn beide konfiguriert sind, hat die Einstellung unter *Computerkonfiguration* Vorrang.

Sicherheitslücken

Ein Angreifer, der administrative Privilegien auf einem Server erlangt hat, könnte das Remoteüberwachungs-Feature ausnutzen, um die Aktivitäten von Benutzern zu verfolgen. Dies könnte zum Verlust vertraulicher Informationen führen. Der Wert möglicher Gegenmaßnahmen ist allerdings gering, da ein Angreifer, der administrative Rechte erlangt hat, die vollständige Kontrolle über den Computer übernommen hat.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** und **Keine Remoteüberwachung erlaubt**.

Mögliche Auswirkungen

Administratoren sind nicht in der Lage, die Remoteüberwachung zu verwenden. Sie können Terminalserver-Benutzern keine Unterstützung bieten.

Die Datenumleitungs-Einstellungen können Sie über den folgenden Pfad konfigurieren: *Computerkonfiguration\Administrative Vorlagen\Windows Komponenten\Terminaldienste\Client/Server-Datenumleitung*

Zeitzonenumleitung zulassen

Diese Einstellung definiert, ob es dem Clientcomputer gestattet ist, seine Zeitzoneneinstellungen auf die Terminalserver-Sitzung umzuleiten. Als Standard ist die Einstellung deaktiviert. Die Zeitzone der Sitzung ist somit dieselbe, wie die des Terminalservers. Der Client kann seine Zeitzone nicht umleiten. Im Moment ist eine Umleitung nur über eine Remotedesktopverbindung oder mit Windows CE 5.1 möglich. Die Konsolensitzung verwendet immer die Einstellungen des Servers. Wenn die Einstellung vom Administrator geändert wird, betrifft dies nur neue Sitzungen. Bestehende Sitzungen werden nicht beeinflusst.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Eine Zeitzonenumleitung ist nur mit einem Windows Terminalserver möglich.

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Deaktiviert**.

Mögliche Auswirkungen

Eine Zeitzonenumleitung ist nicht möglich.

Zwischenablageumleitung nicht zulassen

Diese Einstellung legt fest, ob die Umleitung der Zwischenablage gestattet ist. Als Standard ist sie deaktiviert. Dies ermöglicht die Umleitung der Zwischenablage.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Eine Umleitung der Zwischenablage ist nicht möglich.

Audioumleitung zulassen

Diese Einstellung legt fest, ob der Benutzer die Audioausgaben der Terminalsitzung auf dem lokalen Computer abspielen kann. Als Standard ist sie deaktiviert. Dies gestattet den Benutzern nicht die Audioausgaben umzuleiten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Eine Umleitung der Audioausgaben ist nicht möglich.

COM-Anschlussumleitung nicht zulassen

Dieser Einstellung legt fest, ob die Umleitung von Daten an die COM-Ports des Clients in der Terminalsitzung möglich ist. Als Standard ist die Einstellung deaktiviert. Dies verhindert, dass Serverdaten auf lokale COM-Ports umgeleitet werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Eine Umleitung der COM-Ports ist nicht möglich.

Clientdruckerumleitung nicht zulassen

Diese Einstellung legt fest, ob die Umleitung von Druckern des Clients an die Terminalsitzung möglich ist. Als Standard ist die Einstellung deaktiviert. Dies ermöglicht, dass lokale Drucker umgeleitet werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Eine Umleitung der Drucker ist nicht möglich.

LPT-Anschlussumleitung nicht zulassen

Diese Einstellung legt fest, ob die Umleitung von LPT-Anschlüssen des Clients an die Terminalsitzung möglich ist. Als Standard ist die Einstellung deaktiviert. Dies ermöglicht, dass die LPT-Anschlüsse umgeleitet werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Eine Umleitung der LPT-Anschlüsse ist nicht möglich.

Laufwerkumleitung nicht zulassen

Als Standard werden die Clientlaufwerke automatisch bei einer Verbindung gemappt. Sie tauchen in der Ordernstruktur der Sitzung im Windows Explorer unter dem Format <*Laufwerksbuchstabe*> auf <C*omputername*> auf. Wenn Sie die Einstellung aktivieren, wird dies verhindert.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Eine Umleitung der Laufwerke ist nicht möglich.

Standardclientdrucker nicht als Standarddrucker in einer Sitzung festlegen

Über diese Einstellung kann verhindert werden, dass der lokale Standarddrucker der Standarddrucker der Terminalsitzung wird. Als Standard ist diese Einstellung deaktiviert. Damit ist der Standarddrucker der gleiche, wie der des lokalen Clients.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Der Standarddrucker des Clients wird nicht der Standarddrucker der Terminalsitzung.

Die Verschlüsselungs- und Sitzungseinstellungen können Sie über den folgenden Pfad festlegen:
Computerkonfiguration\Administrative Vorlagen\Windows Komponenten\Terminaldienste\Verschlüsselung und Sicherheit

Verschlüsselungsstufe der Clientverbindung festlegen

Diese Einstellung legt fest, ob eine Verschlüsselung für eine Terminalsitzung durchgesetzt wird. Wenn sie aktiviert ist, können Sie eine Verschlüsselungsstufe festlegen. Die Standardeinstellung ist **Hohe Verschlüsselung**.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Kompatibel:** Die Sitzung wird in beide Richtungen mit dem stärksten vom Client unterstützten Schlüssel verschlüsselt. Verwenden Sie die Option, wenn in der Umgebung ältere Clients vorhanden sind.
  - **Hohe Verschlüsselung:** Die Sitzung wird in beide Richtung mit einem 128-Bit Schlüssel verschlüsselt. Verwenden Sie die Option, wenn in Ihrer Umgebung nur 128-Bit Clients vorhanden sind. Zum Beispiel Remotedesktopverbindungs-Clients. Clients, die eine solche Verschlüsselung nicht unterstützen, können keine Verbindung aufbauen.
  - **Geringe Verschlüsselung**: Nur die Daten, die vom Client zum Server gesendet werden, werden mit einem 56-Bit Schlüssel verschlüsselt. Die Daten vom Server zum Client werden nicht verschlüsselt.
- **Deaktiviert**
- **Nicht konfiguriert**

Wichtig: Wenn die Einstellung Systemkryptografie: **FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden** aktiviert wurde, können Sie über die Einstellung **Verschlüsselungsstufe der Clientverbindung festlegen** die Verschlüsselungsstufe nicht ändern.

Sicherheitslücken

Wenn es den Clients möglich ist, eine Sitzung mit geringer Verschlüsselung aufzubauen, hat ein Angreifer eine bessere Chance den Netzwerkverkehr zu entschlüsseln.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Hohe Verschlüsselung**.

Mögliche Auswirkungen

Clients, die eine 128-Bit Verschlüsselung nicht unterstützen, können keine Terminalsitzung aufbauen.

Clients bei der Verbindungsherstellung immer zur Kennworteingabe auffordern

Wenn diese Einstellung aktiviert ist, muss der Benutzer bei jeder Verbindung ein Passwort eingeben – auch wenn dieser bereits im Remotedesktop-Client ein Passwort angegeben hat.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzername und Passwort können beide vom Benutzer im Remotedesktop-Client gespeichert werden. Wenn ein Angreifer dann auf diesen Client Zugriff erlangt hat, und eine erneute Eingabe des Passwortes bei einer Verbindung nicht erzwungen wird, hat der Angreifer die Möglichkeit eine Terminalsitzung aufzubauen – auch wenn er das Passwort des Benutzers tatsächlich gar nicht kennt.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Die Benutzer müssen bei jeder neuen Terminalsitzung ein Passwort angeben.

Sie können Sie RPC-Sicherheitseinstellung für Terminalserver über den folgenden Pfad konfigurieren: *Computerkonfiguration\Administrative Vorlagen\Windows Komponenten\Terminaldienste\Verschlüsselung und Sicherheit\RPC Sicherheit*

Sicherer Server (Sicherheit erforderlich)

Wenn diese Einstellung aktiviert ist, legt dies fest, dass der Terminalserver eine sichere Remote Procedure Call (RPC)-Kommunikation mit den Clients erfordert. Wenn sie deaktiviert ist, fordert der Terminalserver zwar immer eine sichere Kommunikation an, akzeptiert jedoch auch eine ungesicherte Kommunikation.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Verwenden Sie für die Administration und Konfiguration der Terminaldienste die RPC-Schnittstelle.

Sicherheitslücken

Wenn eine ungesicherte RPC-Kommunikation möglich ist, wird der Server für Man-in-the-middle-Angriffe verwundbar. Ein Man-in-the-middle-Angriff findet statt, wenn ein Eindringling Pakete zwischen Client und Server abfängt, und diese vor deren Weiterleitung verändert. Meist wird versucht, über diese Änderungen den Client oder den Server zur Bekanntgabe von sensiblen Informationen zu bringen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Clients, die sicheres RPC nicht unterstützen, sind nicht in der Lage den Server remote zu verwalten.

Die RPC-Sicherheitseinstellungen für Terminalserver können Sie über den folgenden Pfad festlegen: *Computerkonfiguration\Administrative Vorlagen\Windows Komponenten\Terminaldienste\Verschlüsselung und Sicherheit\RPC Sicherheit\Sitzungen*

Zeitlimit für getrennte Sitzungen festlegen

Diese Einstellung legt fest, wie lange eine getrennte Sitzung auf dem Server aktiv bleibt. Als Standard ist es Benutzern möglich, eine Terminalsitzung ohne Abmeldung zu beenden. In diesem Status werden die Programme in der Sitzung weiter ausgeführt, auch wenn der Benutzer nicht mehr verbunden ist. Normalerweise werden diese Sitzungen ohne Zeitlimit weitergeführt. Wenn die Einstellung aktiviert ist, werden sie nach einer bestimmten Zeit getrennt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Nie**
  - **1 Minute**
  - **5 Minuten**
  - **10 Minuten**
  - **15 Minuten**
  - **30 Minuten**
  - **1 Stunde**
  - **2 Stunden**
  - **3 Stunden**
  - **1 Tag**
  - **2 Tage**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Diese Einstellung wirkt sich auf Konsolensitzungen, wie zum Beispiel Remotedesktopverbindungen, nicht aus. Sie steht unter *Computerkonfiguration* und unter *Benutzerkonfiguration* zur Verfügung. Wenn beide konfiguriert sind, hat die Einstellung unter *Computerkonfiguration* Vorrang.

Sicherheitslücken

Jede Terminalserver-Sitzung verbraucht Systemressourcen. Wenn getrennte Sitzungen nicht nach einer bestimmten Zeit beendet werden, könnten dem Server die Ressourcen ausgehen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** und **1 Tag**.

Mögliche Auswirkungen

Sitzungen von Benutzern, die vergessen sich abzumelden, werden nach 24 Stunden Inaktivität beendet.

Erneute Verbindung nur vom ursprünglichen Client zulassen

Wenn diese Einstellung aktiviert ist, wird verhindert, dass Benutzer eine neue Verbindung zu einer

bestehenden Sitzung über einen anderen Client aufbauen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Wichtig: Diese Einstellung wird nur für Citrix ICA Clients unterstützt, die bei einer Verbindung eine Seriennummer zur Verfügung stellen. Wenn Benutzer eine Verbindung über einen Windows-Client aufbauen, wird sie ignoriert. Sie steht unter *Computerkonfiguration* und unter *Benutzerkonfiguration* zur Verfügung. Wenn beide konfiguriert sind, hat die Einstellung unter *Computerkonfiguration* Vorrang.

Sicherheitslücken

Normalerweise können Benutzer eine Terminalsitzung von jedem Computer aus fortsetzen. Diese Einstellung verhindert das. Ihr Wert ist eher gering, da sie nur für Benutzer von Citrix ICA Clients durchgesetzt wird.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer, die eine Verbindung über Citrix ICA Clients aufbauen, können eine bestehende Sitzung nur von dem Client aus weiterführen, von dem aus diese aufgebaut wurde.

Internetinformationsdienste

IIS 6.0 (Internet Information Services), der von Windows Server 2003 zur Verfügung gestellte Webserver, ermöglicht eine einfache Veröffentlichung von Dokumenten und Informationen im Intranet und Internet. Sie können die IIS-Einstellung über den folgenden Pfad konfigurieren: *Computerkonfiguration\Administrative Vorlagen\Windows Komponenten\Internetinformationsdienste*

IIS-Installation verhindern

Die IIS 6.0 sind als Standard unter Windows Server 2003 nicht installiert. Wenn die Einstellung aktiviert ist, können sie auch später nicht installiert werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

In den vorhergehenden Versionen der IIS und den von ihnen abhängigen Anwendungen gab es einige Sicherheitslöcher. Obwohl die IIS 6.0 sicherer als ihre Vorgänger sind, ist es natürlich möglich, dass es bis jetzt unentdeckte Sicherheitslöcher gibt. Daher möchten Organisationen möglicherweise

sicherstellen, dass diese auf Nicht-Webservern nicht installiert werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Sie sind nicht in der Lage, Windows Komponenten oder Anwendungen zu installieren, die die IIS benötigen. Es wird bei einem solchen Versuch keine Fehlermeldung angezeigt. Wenn die IIS bereits installiert sind, hat dieser Einstellung keine Auswirkungen.

Windows Update

Windows Update wird für das Herunterladen von Security-Fixes, kritischen Updates und den aktuellsten Hilfedateien, Treibern und Internetprodukten verwendet. Sie können Windows Update über den folgenden Pfad konfigurieren:
Computerkonfiguration\Administrative Vorlagen\Windows Komponenten\Windows Update

Automatische Updates konfigurieren

Wenn diese Einstellung aktiviert ist, verwenden die Computer Ihrer Umgebung automatische Updates. Wenn sie deaktiviert ist, müssen Sie die verfügbaren Updates manuell von der Windows Update Webseite unter http://windowsupdate.microsoft.com herunterladen. Administratoren können die automatischen Updates allerdings weiterhin über die Systemsteuerung konfigurieren.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **2: Vor dem Herunterladen und dem Installieren von Updates benachrichtigen.**
  - **3: Updates automatisch herunterladen und vor der Installation benachrichtigen.** Dies ist die Standardeinstellung.
  - **4: Updates automatisch herunterladen und diese nach dem definierten Zeitplan installieren.** Wenn kein Zeitplan konfiguriert ist, wird die Installation täglich um 3:00 Uhr nachts durchgeführt. Wenn für die Fertigstellung der Installation Neustarts erforderlich sind, werden diese automatisch durchgeführt. Sollte ein Benutzer angemeldet sein, wird dieser benachrichtigt und kann den Neustart verzögern.
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn das automatische Update aktiviert ist, verfügen die Computer ihrer Organisation immer über die neusten Updates und Servicepacks. So werden Sicherheitslücken schnellstmöglich geschlossen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** und wählen Sie die Option **4 = Updates automatische herunterladen und diese nach dem definierten Zeitplan installieren**.

Mögliche Auswirkungen

Kritische Betriebssystemupdates und Servicepacks werden automatisch heruntergeladen und täglich um 3:00 Uhr nachts installiert.

Kein automatischer Neustart für geplante Installationen automatischer Updates

Wenn die Einstellung aktiviert ist, wird kein automatischer Neustart nach der Installation von Updates ausgeführt – auch dann nicht, wenn ein Benutzer angemeldet ist. Stattdessen benachrichtigt das automatische Update den Benutzer darüber, dass er den Computer neu starten muss um die Installation abzuschließen. Bedenken Sie, dass weitere Updates erst nach dem Neustart erkannt und installiert werden. Wenn die Einstellung deaktiviert ist, wird der Computer nach der Benachrichtigung des Benutzers nach 5 Minuten neu gestartet.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Dieser Einstellung ist nur wirksam, wenn die Einstellung **Automatische Updates konfigurieren** für eine geplante Installation konfiguriert ist.

Sicherheitslücken

Manchmal muss für die Fertigstellung von Updates das Betriebssystem neu gestartet werden. Wenn dies nicht durchgeführt wird, ist das aktuelle Update nicht vollständig installiert, und neue Updates werden nicht erkannt und installiert.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Deaktiviert**.

Mögliche Auswirkungen

Es gibt einen ernsten Nachteil bei der Aktivierung dieser Einstellung. Ein automatischer Neustart wird auch auf den Servern durchgeführt. Bei kritischen Servern kann das zu einem unerwarteten temporären DoS-Zustand führen.

Geplante Installationen automatischer Updates erneut planen

Diese Einstellung legt den Zeitraum fest, den das automatische Update nach dem Systemstart wartet, bevor eine fehlgeschlagene Installation erneut durchgeführt wird. Wenn sie aktiviert ist, wird die Installation nach dem konfigurierten Zeitraum erneut durchgeführt. Ist sie deaktiviert, wird diese erst mit der nächsten geplanten Installation durchgeführt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert:** Ein benutzerdefinierter Wert zwischen **1** und **60** Minuten.
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Dieser Einstellung wirkt sich nur aus, wenn die Einstellung **Automatische Updates konfigurieren** für die geplante Installation konfiguriert ist. Ansonsten hat sie keinen Effekt.

Sicherheitslücken

Wenn nicht vor der nächsten Installation ein paar Minuten abgewartet wird, könnte dieses zu Konflikten mit beim Systemstart noch nicht vollständig gestarteten Anwendungen und Diensten führen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** und **10 Minuten**.

Mögliche Auswirkungen

Automatische Updates werden erst 10 Minuten nach dem Neustart des Computers durchgeführt.

Internen Pfad für den Microsoft Updatedienst angeben

Wenn dieser Einstellung aktiviert ist, legt sie einen Intranet-Server fest, der Updates der Microsoft Update Webseite zur Verfügung stellt. Dieser wird dann, anstelle der Microsoft Update Webseite, von den Computern Ihres Netzwerkes auf verfügbare Updates abgefragt. Damit Sie diese Einstellung verwenden können, müssen Sie zwei Servernamen angeben: Den Server, von dem die Update-Clients ihre Updates abfragen und erhalten, und den Server auf den die aktualisierten Uploadstatistiken der Arbeitsstationen hochgeladen werden. Sie können den gleichen Server für beide Funktionen verwenden. Auf diese Weise müssen Updateverbindungen nicht über eine Firewall aufgebaut werden, und Sie haben die Möglichkeit, die Updates vor deren Bereitstellung zu testen.

Die möglichen Werte für diese Einstellung sind:^

- **Aktiviert:** Wenn Sie dieser Einstellung verwenden, definieren Sie im Dialogfenster **Eigenschaften** die Namen des Updateservers und des Statistikservers.
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Wenn die Einstellung **Automatische Updates konfigurieren** deaktiviert ist, hat diese Einstellung keine Auswirkungen.

Sicherheitslücken

Einige Organisationen möchten Updates möglicherweise vor einer Bereitstellung testen. Außerdem wird der Verkehr auf den Firewalls, Routern und Proxy-Servern verringert, da die Updates nun nicht mehr von der Microsoft Webseite, sondern von dem internen SUS-Server (Software Update Services) heruntergeladen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**. Geben Sie dann die entsprechenden Servernamen an.

Mögliche Auswirkungen

Kritische Updates und Servicepacks werden von den IT-Mitarbeitern der Organisation verwaltet.

Anmeldeeinstellungen

Diese Einstellungen beeinflussen die Anmeldung der Benutzer. Sie können sie unter dem folgenden Pfad konfigurieren:
Computerkonfiguration\Administrative Vorlagen\System\Anmeldung

Willkommenseite für "Erste Schritte" bei der Anmeldung nicht anzeigen

Diese Einstellung verhindert die Anzeige des Willkommensbildschirms von Microsoft Windows® 2000 Professional und Windows XP Professional. Sie betrifft nur Windows 2000 Professional und Windows XP Professional.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Diese Einstellung steht sowohl unter *Computerkonfiguration*, als auch unter *Benutzerkonfiguration* zur Verfügung. Wenn beide konfiguriert sind, hat die Einstellung unter *Computerkonfiguration* Vorrang.

Sicherheitslücken

Der Willkommensbildschirm ermöglicht es dem Benutzer den Windows XP Desktop kennen zu lernen. Einige Organisationen möchten dies möglicherweise nicht, da sie dem Benutzer andere Möglichkeiten der Schulung bieten.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Der Willkommensbildschirm wir den Benutzern nicht angezeigt.

Microsoft Office XP Custom Maintenance Wizard

Der Microsoft Office XP Custom Maintenance Wizard (Microsoft Office XP Anpassungsassistent) ermöglicht es Ihnen, die auf den Benutzercomputern installierten Features von Softwareprodukten zu aktualisieren. Der Assistent liest als erstes das Windows Installer Paket (.msi Datei) und erstellt dann eine neue Produktkonfigurationsdatei (.cmw). Danach verwendet er die .cmw-Datei, um die installierten Features auf den Computern der Benutzer zu aktualisieren.

Die administrativen Vorlagen (.adm) für Office XP sind unter Windows XP oder Windows Server 2003 normalerweise nicht vorhanden. Sie sind in den Office XP Resource Kit Tools enthalten. Diese können Sie unter http://www.microsoft.com/office/ork/xp/appndx/appa18.htm (englischsprachig) herunterladen. Nach der Installation der Tools finden Sie im Ordner %systemroot%\inf die folgenden Vorlagen:

- Access10.adm enthält die Einstellungen für Access 2002.
- Excel0.adm enthält die Einstellungen für Excel 2002.
- FP10.adm enthält die Einstellungen für Microsoft Front Page® 2002.
- GAL.adm enthält die Einstellungen für die Office XP Zwischenablage.
- Instlr11.adm enthält die Einstellungen für den Windows Installer.
- Office10.adm Einstellungen die für alle Office XP Anwendungen gelten.
- Outlk10.adm enthält die Einstellungen für Microsoft Outlook® 2002.
- Ppt10.adm enthält die Einstellungen für Microsoft PowerPoint® 2002.
- Pub10.adm enthält die Einstellungen für Publisher 2002.
- Word10.adm, enthält die Einstellungen für Word 2002.

► Um die .adm-Vorlagen im Snap-In Gruppenrichtlinie zu importieren

1. Klicken Sie mit der rechten Maustaste auf **Administrative Vorlagen** und dann auf **Administrative Vorlage hinzufügen/entfernen**.
2. Klicken Sie auf **Hinzufügen**
3. Wählen Sie die entsprechende .adm-Vorlage aus.

Die neuen Richtlinien werden in den entsprechenden Pfaden der Gruppenrichtlinie angezeigt.

Die Einstellungen des **Microsoft Office XP Custom Maintenance Wizard** können Sie unter dem folgenden Pfad konfigurieren:
Computerkonfiguration\Administrative Vorlagen\Microsoft Office XP\Custom Maintenance Wizard

Anwendung aller CMW-Dateien erlauben

Wenn der Benutzer nicht Administrator des Computers ist, müssen die CMW-Dateien in den CMW-Ordner, der durch die Sourcelist der Windows Installers definierten Installationsquelle der Anwendung, platziert werden. Über diese Einstellung können Sie dieses Verhalten ändern.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Ein böswilliger Benutzer, der seinen eigenen CMW-Ordner anpassen kann, könnte nicht autorisierte Softwarepakete auf dem Computer installieren.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Benutzer können nur aus den Quellen installieren, die in der Office XP Sourcelist des Windows

Installer definiert sind.

Microsoft Office XP Sicherheitseinstellungen

Microsoft Office XP umfasste einige Sicherheitsfeatures, die für eine starke Sicherheit bei gleichzeitiger Flexibilität sorgen. Sie können die Microsoft Office XP Sicherheitseinstellungen über den folgenden Pfad konfigurieren:
Computerkonfiguration\Administrative Vorlagen\Microsoft Office XP\ Security Settings

Access: Allen installierten Add-ins und Vorlagen vertrauen

Unter Microsoft Access wird diese Einstellung nur für COM Add-ins verwendet.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Sie haben die Möglichkeit allen momentan installierten Add-Ins und Vorlagen zu vertrauen. Damit wird allen mit Microsoft Office installierten Dateien vertraut - unabhängig davon, ob diese signiert sind oder nicht. Es ist möglich, dass ein Angriff über einen Virus, ein Trojanisches Pferd oder anderen feindlichen Code eingebettet in ein Office-Dokument, stattfindet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Es gibt keinen direkten Weg, im Voraus eine Liste von vertrauenswürdigen Quellen zu laden. Sie müssen jedes Zertifikat erst auf einem Testcomputer akzeptieren. Dies kann viel Zeit in Anspruch nehmen.

VBA für Office-Anwendungen deaktivieren

Diese Einstellung verhindert, das Excel, FrontPage, Outlook, PowerPoint, Microsoft Publisher und Word Microsoft Visual Basic® for Applications (VBA) verwenden. Durch diese Einstellung werden keine VBA-Dateien auf dem Computer installiert oder entfernt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

VBA wird von einigen Administratoren als Sicherheitsrisiko betrachtet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

VBA steht nicht zur Verfügung. Daher können Makros, Scripts und andere Anwendungen, die von VBA abhängig sind, fehlschlagen.

Excel: Makro-Sicherheitsebene

Über diese Einstellung können Sie den Makrovirusschutz konfigurieren.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Hoch**
    - **Unsignierte Makros**: Makros sind automatisch deaktiviert, und die Datei wird geöffnet.
    - **Signierte Makros:** Die Quelle und die Signatur des Makros legen fest, wie dieses gehandhabt wird.
    - **Vertrauenswürdige Quelle:** Signatur ist gültig: Makros sind automatisch aktiviert und die Datei wird geöffnet.
    - **Unbekannter Autor:** Signatur ist gültig: Es wird ein Dialogfenster mit den Zertifikatsinformationen angezeigt. Makros können nur dann aktiviert werden, wenn der Benutzer dem Autor und der Zertifizierungsstelle vertraut. Ein Netzwerkadministrator kann die Liste der vertrauenswürdigen Quellen sperren und damit verhindern, dass der Benutzer diese erweitert.
    - **Jeder Autor:** Signatur ist ungültig – möglicherweise aufgrund eines Virus. Der Benutzer wird vor einem möglichen Virus gewarnt. Makros sind automatisch deaktiviert.
    - **Jeder Autor:** Signaturprüfung ist nicht möglich, da der öffentliche Schlüssel fehlt oder ein inkompatibles Verschlüsselungsverfahren verwendet wurde. Der Benutzer wird gewarnt, dass eine Signaturprüfung nicht möglich ist. Makros sind automatisch deaktiviert.
    - **Jeder Autor:** Die Signatur wurde erstellt, nachdem das Zertifikat abgelaufen war oder zurückgezogen wurde. Der Benutzer wird gewarnt, dass die Signatur abgelaufen ist oder zurückgezogen wurde. Makros sind automatisch deaktiviert.
  - **Medium**
    - **Unsignierte Makros:** Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
    - **Signierte Makros:** Die Quelle und die Signatur des Makros legen fest, wie dieses gehandhabt wird.
    - **Vertrauenswürdige Quelle:** Signatur ist gültig: Makros sind automatisch aktiviert, und die Datei wird geöffnet.
    - **Unbekannter Autor:** Signatur ist gültig: Es wird ein Dialogfenster mit den Zertifikatsinformationen angezeigt. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren. Er kann dem Ersteller und der Zertifizierungsstelle vertrauen oder auch nicht.

        - **Jeder Autor:** Signatur ist ungültig – möglicherweise aufgrund eines Virus. Der Benutzer wird vor einem möglichen Virus gewarnt. Makros sind automatisch deaktiviert.
        - **Jeder Autor:** Signaturprüfung ist nicht möglich, da der öffentliche Schlüssel fehlt oder ein inkompatibles Verschlüsselungsverfahren verwendet wurde. Der Benutzer wird gewarnt, dass eine Signaturprüfung nicht möglich ist. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
        - **Jeder Autor:** Die Signatur wurde erstellt, nachdem das Zertifikat abgelaufen war oder zurückgezogen wurde. Der Benutzer wird gewarnt, dass die Signatur abgelaufen ist oder zurückgezogen wurde. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
    - **Low:** Alle Makros werden gleich behandelt – unabhängig von deren Quelle und Status. Es gibt keine Benachrichtigungen oder Signaturüberprüfungen. Makros werden automatisch aktiviert. Verwenden Sie die Einstellung nur, wenn Sie sicher sind, dass die Makros aller Dateien aus vertrauenswürdigen Quellen stammen.
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

In der Vergangenheit gab es viele Viren und Würmer, die als Makros in Office-Dokumenten entwickelt wurden. Ein Wurm ist ein Programm, das unabhängig arbeitet und sich über Netzwerkverbindungen von Computer zu Computer verbreitet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Medium**.

Mögliche Auswirkungen

Benutzern wird bei jedem Laden von unsignierten Makros oder bei signierten Makros, bei denen ein Problem mit dem Autor oder dem Zertifikat besteht, eine Fehlermeldung angezeigt. Makros mit ungültigen Signaturen werden deaktiviert.

Excel: Zugriff auf Visual Basic Project gestatten

Diese Einstellung legt fest, ob Excel Zugriff auf den VBA-Code von Dokumenten hat.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wie bei Makros auch, kann der VBA-Code Viren und Würmer enthalten.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

VBA-Code in Office-Dokumenten wird nicht ausgeführt.

Excel: Installierten Add-ins und Vorlagen vertrauen

Abhängig von den Makro-Sicherheitseinstellungen, wird ein Makro beim Öffnen deaktiviert, und Sie erhalten eine Mitteilung. Alle Makros, die mit Office XP installiert werden, sind von Microsoft signiert. Nachdem Sie für eins dieser Makros Microsoft zur Liste der vertrauenswürdigen Quellen hinzugefügt haben und die Einstellung **Excel: Installierten Add-ins und Vorlagen vertrauen** aktiviert haben, sollte bei deren Verwendung keine Benachrichtigung mehr auftreten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Sie haben die Möglichkeit, allen momentan installierten Add-Ins und Vorlagen zu vertrauen. Damit wird allen mit Microsoft Office installierten Dateien vertraut - unabhängig davon, ob diese signiert sind oder nicht. Es ist möglich, dass ein Angriff über einen Virus, ein Trojanisches Pferd oder anderen feindlichen Code eingebettet in ein Office-Dokument, stattfindet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Es gibt keinen direkten Weg, im Voraus eine Liste von vertrauenswürdigen Quellen zu laden. Sie müssen jedes Zertifikat erst auf einem Testcomputer akzeptieren. Dies kann viel Zeit in Anspruch nehmen.

Outlook: Makro Sicherheitsebene

E-Mails, die Sie auf Ihrem Computer erhalten, könnten Makros und Scripts mit Viren enthalten. Um Ihren Computer gegen solche Viren zu schützen, ist die Standard-Sicherheitseinstellung von Outlook **Hoch**.

Die möglichen Werte dieser Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
    - **Hoch:** Dies ist die Standardeinstellung. Sie können nur Makros ausführen, die signiert sind und aus einer vertrauenswürdigen Quelle stammen. Bevor Sie einer Quelle vertrauen, sollten Sie deren Arbeitsweise überprüfen, da Outlook Makros aus vertrauenswürdigen Quellen ohne jede Warnung ausführt.
    - **Mittel:** Bei einem Makro aus einer Quelle, die nicht in Ihrer Liste vertrauenswürdigen Quellen steht, zeigt Outlook eine Warnmeldung an. Sie können dies dann aktivieren oder deaktivieren.

    - **Gering:** Wählen Sie diese Einstellung nur, wenn Sie sicher sind, dass alle von Ihnen geöffneten Makros sicher sind. Sie stellt den Makroschutz von Outlook aus. Alle Makros werden ausgeführt.
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Outlook ist nicht in der Lage, Disketten, Festplatten oder Netzlaufwerke auf Makroviren zu prüfen. Wenn Sie eine solche Funktionalität benötigen, müssen Sie einen Virenscanner einsetzen.

Sicherheitslücken

In der Vergangenheit gab es viele Viren und Würmer, die als Makros in Office-Dokumenten entwickelt wurden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **High**.

Mögliche Auswirkungen

Nur signierte Makros aus vertrauenswürdigen Quellen werden ausgeführt.

PowerPoint: Makro Sicherheitsebene

Diese Einstellung legt den Virenschutz in PowerPoint fest.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
    - **Hoch**
        - **Unsignierte Makros**: Makros sind automatisch deaktiviert und die Datei wird geöffnet.
        - **Signierte Makros:** Die Quelle und die Signatur des Makros legen fest, wie dieses gehandhabt wird.
        - **Vertrauenswürdige Quelle:** Signatur ist gültig: Makros sind automatisch aktiviert und die Datei wird geöffnet.
        - **Unbekannter Autor:** Signatur ist gültig: Es wird ein Dialogfenster mit den Zertifikatsinformationen angezeigt. Makros können nur dann aktiviert werden, wenn der Benutzer dem Autor und der Zertifizierungsstelle vertraut. Ein Netzwerkadministrator kann die Liste der vertrauenswürdigen Quellen sperren, und damit verhindern, dass der Benutzer diese erweitert.
        - **Jeder Autor:** Signatur ist ungültig - möglicherweise aufgrund eines Virus. Der Benutzer wird vor einem möglichen Virus gewarnt. Makros sind automatisch deaktiviert.
        - **Jeder Autor:** Signaturenprüfung ist nicht möglich, da der öffentliche Schlüssel fehlt oder ein inkompatibles Verschlüsselungsverfahren verwendet wurde. Der Benutzer wird gewarnt, dass eine Signaturprüfung nicht möglich ist. Makros sind automatisch deaktiviert.
        - **Jeder Autor:** Die Signatur wurde erstellt, nachdem das Zertifikat abgelaufen war oder zurückgezogen wurde. Der Benutzer wird gewarnt, dass die Signatur abgelaufen ist oder zurückgezogen wurde. Makros sind automatisch deaktiviert.

- **Medium**
  - **Unsignierte Makros:** Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
  - **Signierte Makros:** Die Quelle und die Signatur des Makros legen fest, wie dieses gehandhabt wird.
  - **Vertrauenswürdige Quelle:** Signatur ist gültig: Makros sind automatisch aktiviert und die Datei wird geöffnet.
  - **Unbekannter Autor:** Signatur ist gültig: Es wird ein Dialogfenster mit den Zertifikatsinformationen angezeigt. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren. Er kann dem Ersteller und der Zertifizierungsstelle vertrauen oder auch nicht.
  - **Jeder Autor:** Signatur ist ungültig – möglicherweise aufgrund eines Virus. Der Benutzer wird vor einem möglichen Virus gewarnt. Makros sind automatisch deaktiviert.
  - **Jeder Autor:** Signaturenprüfung ist nicht möglich, da der öffentliche Schlüssel fehlt oder ein inkompatibles Verschlüsselungsverfahren verwendet wurde. Der Benutzer wird gewarnt, dass eine Signaturprüfung nicht möglich ist. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
  - **Jeder Autor:** Die Signatur wurde erstellt, nachdem das Zertifikat abgelaufen war oder zurückgezogen wurde. Der Benutzer wird gewarnt, dass die Signatur abgelaufen ist oder zurückgezogen wurde. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
- **Low:** Alle Makros werden gleich behandelt - unabhängig von deren Quelle und Status. Es gibt keine Benachrichtigungen oder Signaturüberprüfungen. Makros werden automatisch aktiviert. Verwenden Sie die Einstellung nur, wenn Sie sicher sind, dass die Makros aller Dateien aus vertrauenswürdigen Quellen stammen.

- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

In der Vergangenheit gab es viele Viren und Würmer, die als Makros in Office-Dokumenten entwickelt wurden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Medium**.

Mögliche Auswirkungen

Benutzern wird bei jedem Laden von unsignierten Makros oder bei signierten Makros, bei denen ein Problem mit dem Autor oder dem Zertifikat besteht, eine Fehlermeldung angezeigt. Makros mit ungültigen Signaturen werden deaktiviert.

PowerPoint: Zugriff auf Visual Basic Project gestatten

Diese Einstellung legt fest, ob PowerPoint Zugriff auf den VBA-Code von Dokumenten hat.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**

- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wie bei Makros auch, kann der VBA-Code Viren und Würmer enthalten.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

VBA-Code in Office-Dokumenten wird nicht ausgeführt.

PowerPoint: Allen installierten Add-ins und Vorlagen vertrauen

Abhängig von den Makro-Sicherheitseinstellungen wird ein Makro beim Öffnen deaktiviert, und Sie erhalten eine Mitteilung. Alle Makros, die mit Office XP installiert werden, sind von Microsoft signiert. Nachdem Sie für eins dieser Makros Microsoft zur Liste der vertrauenswürdigen Quellen hinzugefügt haben und die Einstellung **PowerPoint: Allen installierten Add-ins und Vorlagen vertrauen** aktiviert haben, sollte bei deren Verwendung keine Benachrichtigung mehr auftreten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Sie haben die Möglichkeit, allen momentan installierten Add-Ins und Vorlagen zu vertrauen. Damit wird allen mit Microsoft Office installierten Dateien vertraut. Ob diese signiert sind oder nicht. Es ist möglich, dass ein Angriff über einen Virus, ein Trojanisches Pferd oder anderen feindlichen Code eingebettet in ein Office-Dokument, stattfindet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Es gibt keinen direkten Weg, im vorab eine Liste von vertrauenswürdigen Quellen zu laden. Sie müssen jedes Zertifikat erst auf einem Testcomputer akzeptieren. Dies kann viel Zeit in Anspruch nehmen.

Unsichere ActiveX-Initialisierung

Über diese Einstellung können Sie festlegen, wie ActiveX-Steuerelemente in Office XP Anwendungen aktiviert werden. ActiveX-Steuerelemente stellen über Office XP und den Internet Explorer

umfangreiche Funktionalität zu Verfügung. Da sie aber ausführbare Codestücke sind, könnte ein böswilliger Entwickler ActiveX-Steuerelemente erstellen, die unerwünschte Aktionen durchführen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Initialize using control defaults** (Initialisierung mit den Standardeinstellung des Steuerelements)
  - **Ask user: persisted data or control defaults** (Benutzerdefiniert: Schreibgeschützte Daten oder Standardeinstellungen des Steuerelements)
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Um gegen schädliche Steuerelemente geschützt zu sein, kann Office XP so konfiguriert werden, dass Endbenutzer nur digital signierte Steuerelemente ausführen können.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** und **Initialize using control defaults.**

Mögliche Auswirkungen

Da die Einstellung bewirkt, dass die durch ein Steuerelement gespeicherten Daten bei jedem Start des Steuerelements verworfen werden, kann Sie zu Problemen beim Anzeigen von Dokumenten führen.

Word: Makro-Sicherheitsebene

Diese Einstellung legt den Virenschutz in Word fest.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Hoch**
    - **Unsignierte Makros**: Makros sind automatisch deaktiviert und die Datei wird geöffnet.
    - **Signierte Makros:** Die Quelle und die Signatur des Makros legen fest, wie dieses gehandhabt wird.
    - **Vertrauenswürdige Quelle:** Signatur ist gültig: Makros sind automatisch aktiviert, und die Datei wird geöffnet.
    - **Unbekannter Autor:** Signatur ist gültig: Es wird ein Dialogfenster mit den Zertifikatsinformationen angezeigt. Makros können nur dann aktiviert werden, wenn der Benutzer dem Autor und der Zertifizierungsstelle vertraut. Ein Netzwerkadministrator kann die Liste der vertrauenswürdigen Quellen sperren und damit verhindern, dass der Benutzer diese erweitert.
    - **Jeder Autor:** Signatur ist ungültig – möglicherweise aufgrund eines Virus. Der Benutzer wird vor einem möglichen Virus gewarnt. Makros sind automatisch deaktiviert.
    - **Jeder Autor:** Signaturprüfung ist nicht möglich, da der öffentliche Schlüssel fehlt oder ein inkompatibles Verschlüsselungsverfahren verwendet wurde. Der Benutzer wird gewarnt, dass eine Signaturprüfung nicht möglich ist. Makros sind automatisch deaktiviert.

        - **Jeder Autor:** Die Signatur wurde erstellt, nachdem das Zertifikat abgelaufen war oder zurückgezogen wurde. Der Benutzer wird gewarnt, dass die Signatur abgelaufen ist oder zurückgezogen wurde. Makros sind automatisch deaktiviert.
    - **Medium**
        - **Unsignierte Makros:** Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
        - **Signierte Makros:** Die Quelle und die Signatur des Makros legen fest, wie dieses gehandhabt wird.
        - **Vertrauenswürdige Quelle:** Signatur ist gültig: Makros sind automatisch aktiviert, und die Datei wird geöffnet.
        - **Unbekannter Autor:** Signatur ist gültig: Es wird ein Dialogfenster mit den Zertifikatsinformationen angezeigt. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren. Er kann dem Ersteller und der Zertifizierungsstelle vertrauen oder auch nicht.
        - **Jeder Autor:** Signatur ist ungültig – möglicherweise aufgrund eines Virus. Der Benutzer wird vor einem möglichen Virus gewarnt. Makros sind automatisch deaktiviert.
        - **Jeder Autor:** Signaturprüfung ist nicht möglich, da der öffentliche Schlüssel fehlt oder ein inkompatibles Verschlüsselungsverfahren verwendet wurde. Der Benutzer wird gewarnt, dass eine Signaturprüfung nicht möglich ist. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
        - **Jeder Autor:** Die Signatur wurde erstellt, nachdem das Zertifikat abgelaufen war oder zurückgezogen wurde. Der Benutzer wird gewarnt, dass die Signatur abgelaufen ist oder zurückgezogen wurde. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
    - **Low:** Alle Makros werden gleich behandelt - unabhängig von deren Quelle und Status. Es gibt keine Benachrichtigungen oder Signaturüberprüfungen. Makros werden automatisch aktiviert. Verwenden Sie die Einstellung nur wenn Sie sicher sind, dass die Makros aller Dateien aus vertrauenswürdigen Quellen stammen.
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

In der Vergangenheit gab es viele Viren und Würmer, die als Makros in Office-Dokumenten entwickelt wurden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Medium**.

Mögliche Auswirkungen

Benutzern wird bei jedem Laden von unsignierten Makros oder bei signierten Makros, bei denen ein Problem mit dem Autor oder dem Zertifikat besteht, eine Fehlermeldung angezeigt. Makros mit ungültigen Signaturen werden deaktiviert.

Word: Allen installierten Add-ins und Vorlagen vertrauen

Abhängig von den Makro-Sicherheitseinstellungen wird ein Makro beim Öffnen deaktiviert und Sie

erhalten eine Mitteilung. Alle Makros, die mit Office XP installiert werden, sind von Microsoft signiert. Nachdem Sie für eins dieser Makros Microsoft zur Liste der vertrauenswürdigen Quellen hinzugefügt haben und die Einstellung **Word: Allen installierten Add-ins und Vorlagen vertrauen** aktiviert haben, sollte bei deren Verwendung keine Benachrichtigung mehr auftreten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Sie haben die Möglichkeit, allen momentan installierten Add-Ins und Vorlagen zu vertrauen. Damit wird allen mit Microsoft Office installierten Dateien vertraut – unabhängig davon, ob diese signiert sind oder nicht. Es ist möglich, dass ein Angriff über einen Virus, ein Trojanisches Pferd oder anderen feindlichen Code eingebettet in ein Office-Dokument, stattfindet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Es gibt keinen direkten Weg, im vorab eine Liste von vertrauenswürdigen Quellen zu laden. Sie müssen jedes Zertifikat erst auf einem Testcomputer akzeptieren. Dies kann viel Zeit in Anspruch nehmen.

Word: Allen installierten Add-ins und Vorlagen vertrauen

Abhängig von den Makro-Sicherheitseinstellungen wird ein Makro beim Öffnen deaktiviert, und Sie erhalten eine Mitteilung. Alle Makros, die mit Office XP installiert werden, sind von Microsoft signiert. Nachdem Sie für eins dieser Makros Microsoft zur Liste der vertrauenswürdigen Quellen hinzugefügt haben und die Einstellung **Word: Allen installierten Add-ins und Vorlagen vertrauen** aktiviert haben, sollte bei deren Verwendung keine Benachrichtigung mehr auftreten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Sie haben die Möglichkeit, allen momentan installierten Add-Ins und Vorlagen zu vertrauen. Damit wird allen mit Microsoft Office installierten Dateien vertraut – unabhängig davon, ob diese signiert sind oder nicht. Es ist möglich, dass ein Angriff über einen Virus, ein Trojanisches Pferd oder anderen feindlichen Code eingebettet in ein Office-Dokument, stattfindet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Es gibt keinen direkten Weg, im vorab eine Liste von vertrauenswürdigen Quellen zu laden. Sie müssen jedes Zertifikat erst auf einem Testcomputer akzeptieren. Dies kann viel Zeit in Anspruch nehmen.

Verarbeitung von Gruppenrichtlinien

Sie können die Verarbeitungsreihenfolge von Gruppenrichtlinien über die Einstellungen im folgenden Pfad anpassen:
Computerkonfiguration\Administrative Vorlagen\System\Gruppenrichtlinien

Verarbeitung von Registrierungsrichtlinien

Diese Einstellung legt fest, wann die Registrierungsrichtlinien aktualisiert werden. Sie betrifft alle Richtlinien im Ordner **administrative Vorlagen** und alle anderen Richtlinien, die Werte der Registrierung ändern. Die Einstellung **Nicht bei der Hintergrundaktualisierung anwenden** verhindert die Hintergrundaktualisierung der Richtlinien. Diese könnte die Arbeit des Benutzers unterbrechen und - in seltenen Fällen - Daten beschädigen. Wenn die Einstellung auf den Wert **Anwenden, auch wenn die Gruppenrichtlinienobjekte nicht geändert wurden** gesetzt ist, werden auch die nicht geänderten Richtlinien neu angewandt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Nicht bei der Hintergrundaktualisierung anwenden**
  - **Anwenden, auch wenn die Gruppenrichtlinienobjekte nicht geändert wurden**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn diese Einstellung auf **Anwenden, auch wenn die Gruppenrichtlinienobjekte nicht geändert wurden** konfiguriert ist, ist sichergestellt, dass die Richtlinien auch dann aktualisiert werden, wenn keine Änderungen vorhanden sind. Auf diese Weise werden alle lokalen Änderungen regelmäßig von den domänenbasierten Gruppernrichtlinien-Einstellungen überschrieben.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** und **Anwenden, auch wenn die Gruppenrichtlinienobjekte nicht geändert wurden**.

Mögliche Auswirkungen

Gruppenrichtlinien werden bei jeder Aktualisierung neu angewandt. Dies könnte geringe Auswirkungen auf die Leistung haben.

Verarbeitung der Richtlinien für die Internet Explorer-Wartung

Diese Einstellung legt fest, wann die Richtlinien für die Internet Explorer-Wartung aktualisiert werden. Sie betrifft alle Richtlinien im Ordner Internet Explorer Maintenance.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
    - **Verarbeitung bei langsamen Netzwerkverbindungen gestatten:** Diese Option aktualisiert die Richtlinien auch dann, wenn diese über eine langsame Netzwerkverbindung übertragen werden. Dies kann zu deutlichen Verzögerungen führen.
    - **Nicht bei der Hintergrundaktualisierung anwenden:** Diese Option verhindert, dass die betroffenen Richtlinien während der Verwendung des Computers aktualisiert werden. Eine Hintergrundaktualisierung könnte zur Unterbrechung der Arbeit des Benutzers führen und - in seltenen Fällen - zu einem Datenverlust.
    - **Anwenden, auch wenn die Gruppenrichtlinienobjekte nicht geändert wurden:** Die Option aktualisiert die Richtlinien und wendet diese neu an. Dies passiert auch dann, wenn sich die Richtlinien nicht geändert haben.
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Indem Sie die Einstellung mit der Option **Process even if the Group Policy objects have not changed** verwenden, stellen Sie sicher, dass die Richtlinien auch dann neu angewandt werden, wenn sich diese nicht verändert haben. So stellen Sie sicher, dass alle lokalen Änderungen von den Gruppenrichtlinien der Domäne überschrieben werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** mit der Option **Process even if the Group Policy objects have not changed**. **Mögliche Auswirkungen**.

Fehlerberichterstattung

Die Fehlerberichterstattung ermöglicht es Administratoren die Cabinet-Dateien, die durch DW.exe erstellt werden zu verwalten und Stop-Fehlermeldung auf einen lokalen Dateiserver umzuleiten. Sie können die Einstellungen der Fehlerberichterstattung über den folgenden Pfad konfigurieren: *Computerkonfiguration\Administrative Vorlagen\System\Fehlerberichterstattung*

Fehlerbenachrichtung anzeigen

Über diese Einstellung können Sie bestimmen, ob dem Benutzer Fehlermeldungen angezeigt werden. Wenn sie aktiviert ist, wird der Benutzer bei Fehlern benachrichtigt und kann selbst auswählen, ob der Fehler weitergeleitet werden soll oder nicht. Ist die Einstellung deaktiviert, kann der Benutzer nicht selbst entscheiden. Die Fehlerberichte werden automatisch weitergeleitet. Wird die Einstellung nicht konfiguriert, kann das Verhalten weiterhin lokal über die Systemsteuerung konfiguriert werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn die Benutzer selbst entscheiden dürfen, ob Fehler weitergeleitet werden, könnten diese Entscheidungen treffen, die nicht mit den Unternehmensrichtlinien übereinstimmen.

Gegenmaßnahmen

Setzen Sie die Einstellungen auf **Deaktiviert**.

Mögliche Auswirkungen

Benutzer werden keine Fehlermeldungen mehr angezeigt.

Fehler melden

Diese Einstellung legt fest, ob Fehler weitergeleitet werden. Wenn sie aktiviert ist, kann der Benutzer entscheiden, ob ein Fehler weitergeleitet wird.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Keine von Microsoft angebotenen Websites bezüglich „weiterer Informationen“ anzeigen.**
  - **Keine zusätzlichen Dateien sammeln.**
  - **Keine zusätzlichen Computerdaten sammeln.**
  - **Warteschlangenmodus für Anwendungsfehler erzwingen:** Mit dieser Option kann der Benutzer nicht mehr wählen, ob er einen Fehlerbericht senden möchte. Stattdessen wird der Fehler an eine Warteschlange gesendet. Der nächste Administrator, der sich anmeldet, muss entscheiden, ob der Fehler gesendet wird.
  - **Dateiuploadpfad für zentrale Fehlerberichte:** Bei dieser Option können Sie einen UNC-Pfad angeben, in den die Fehlerberichte hochgeladen werden.
  - **Instanzen des Worts "Microsoft" ersetzen durch.**
- **Deaktiviert**
- **Nicht konfiguriert**

Wenn diese Einstellung nicht konfiguriert wird, kann der Benutzer sie selbst über die Systemsteuerung konfigurieren.

Sicherheitslücken

Das Fehlerberichterstattungs-Feature von Windows XP, Windows Server 2003 und Office XP sendet normalerweise Daten an Microsoft, die einige Unternehmen lieber vertraulich behandeln möchten. Die Datenschutzvereinbarung von Microsoft stellt sicher, dass Microsoft diese gesammelten Daten nicht missbraucht. Trotzdem mag es sein, das einige Organisationen keine Daten ohne eine vorherige Prüfung durch Mitglieder des IT-Teams senden möchten, andererseits jedoch die Fehlerberichterstattung nicht komplett deaktivierten möchten, da Microsoft die Informationen zur Erkennung und zur Diagnose von Fehlern verwendet. Ein Verfahren, um beides sicherzustellen ist das Einrichten eines internen Fehlerberichterstattungs-Servers (Corporate Error Reporting - CER). Sie können die Clientcomputer dann so konfigurieren, dass diese die Fehlerberichte an den Server senden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert,** und Tragen unter **Dateiuploadpfad für zentrale Fehlerberichte** den UNC-Pfad des CER-Servers ein.

> **Anmerkung:** Weitere Informationen zur Einrichtung von CER-Servern finden Sie auf der Office Resource Kit Webseite unter http://www.microsoft.com/office/ork/xp/appndx/appa19.htm (englischsprachig).

Mögliche Auswirkungen

Die Fehlerberichterstattung ist aktiviert. Die Fehlerberichte werden an den CER-Server gesendet.

Internet Explorer Benutzereinstellungen

Viele der Einstellungen des Internet Explorers können Sie über den folgenden Pfad einer Gruppenrichtlinie konfigurieren:
Benutzerkonfiguration\Administrative Vorlagen\Windows Komponenten\Internet Explorer

Menü "Datei": Menüoption "Speichern unter..." deaktivieren

Die Aktivierung dieser Einstellung verhindert, dass Benutzer Dateien beim Herunterladen speichern können. Die Datei wird nicht heruntergeladen und der Benutzer wird darüber informiert.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten Dateien herunterladen und ausführen, die bösartigen Programmcode enthalten.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht in der Lage Dateien herunterzuladen.

Outlook Express konfigurieren

Diese Einstellung ermöglicht es Administratoren den Benutzern die Möglichkeit zu nehmen, Dateianhänge in Microsoft Outlook® Express zu speichern. Diese könnten zum Beispiel Viren enthalten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit der folgenden Option:**
  - **Anhänge die Viren enthalten können blockieren**

- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer, die E-Mail öffnen, könnten unbeabsichtigt bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** und **Anhänge die Viren enthalten können blockieren**.

Mögliche Auswirkungen

Benutzer sind nicht in der Lage, in Outlook Express Anhänge auszuführen oder zu speichern.

Einstellungen für die Seite "Erweitert" deaktivieren

Diese Einstellung verhindert, dass Benutzer die Einstellungen auf der Seite „Erweitert“ im Dialogfenster „Internetoptionen“ ändern.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Die Benutzer sind nicht in der Lage, die Einstellungen auf der Registerkarte „Erweitert“ im Dialogfenster „Internetoptionen“ zu verändern.

Änderung der Einstellungen für automatische Konfiguration deaktivieren

Diese Einstellung verhindert, dass Benutzer die automatischen Konfigurationseinstellungen verändern. Die automatische Konfiguration ist ein Verfahren, über das Administratoren die Browsereinstellungen regelmäßig aktualisieren können. Sie finden diese im Bereich *Automatische Konfiguration* des Dialogfensters **Local Area Network (LAN) Einstellungen**.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**

- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Die Benutzer sind nicht in der Lage, die Einstellungen für die automatische Konfiguration zu verändern.

Änderung der Zertifikateinstellungen deaktivieren

Diese Einstellung verhindert, dass Benutzer die Zertifikatseinstellung des Internet Explorers ändern. Zertifikate werden verwendet, um die Identität von Softwareanbietern zu prüfen. Wenn die Einstellung aktiviert ist, kann der Benutzer auf die Registerkarte *Inhalte* des Dialogfensters *Internetoptionen* auf den Bereich *Zertifikate* nicht mehr zugreifen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Achtung: Die Aktivierung dieser Richtlinie verhindert nicht, das Benutzer den Zertifikatsverwaltungsassistenten ausführen, indem sie doppelt auf eine Zertifikatskonfigurationsdateien (.spc) klicken. Dieser Assistent ermöglicht es Benutzern, die Einstellungen für neue Zertifikate zu konfigurieren.

Sicherheitslücken

Benutzer könnten neue Zertifikate importieren, bestätigte Zertifikate entfernen, oder deren Einstellungen verändern. Dies könnte zum Fehlschlag von bestätigten Anwendungen oder der Ausführung von nicht bestätigten Anwendungen führen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die Zertifikatseinstellungen zu verändern.

Änderung der Verbindungseinstellungen deaktivieren

Diese Einstellung verhindert, dass Benutzer die Einstellungen der Einwählverbindungen ändern. Wenn die Einstellung aktiviert ist, kann der Benutzer auf die Registerkarte *Verbindungen* des Dialogfensters *Internetoptionen* nicht mehr zugreifen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer können bestehende Verbindungen verändern und so den Zugriff auf Webseiten verhindern.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die Verbindungseinstellungen zu verändern.

Änderung der Proxy-Einstellungen deaktivieren

Diese Einstellung verhindert, dass Benutzer die Proxy-Einstellungen ändern.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer können bestehende Proxy-Einstellungen verändern und so den Zugriff auf Webseiten verhindern.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die Proxy-Einstellungen zu verändern.

Assistenten für Internetzugang deaktivieren

Diese Einstellung verhindert, dass Benutzer den Internetverbindungsassistenten ausführen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer können über den Internetverbindungsassistenten neue Internetverbindungen erstellen. So könnte das Unternehmensnetzwerk angreifbar werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer können den Internetverbindungsassistenten nicht verwenden.

Kennwörter in AutoVervollständigen können nicht gespeichert werden

Diese Einstellung deaktiviert die automatische Vervollständigung von Benutzernamen und Passwörtern in Formularen auf Webseiten. Außerdem werden die Benutzer nicht mehr gefragt, ob sie Passwörter speichern möchten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Das AutoVervollständigen Feature ist sehr nützlich. Es speichert Passwörter in geschütztem Speicher. Hierbei handelt es sich zwar um einen sehr sicheren Schutz, per Definition muss die gespeicherte Information jedoch mindestens für denjenigen abrufbar sein, der sie gespeichert hat. Es gibt inzwischen Tools im Internet, die den Inhalt des geschützten Speichers des Benutzers anzeigen. Sie können zwar nicht verwendet werden, um den Inhalt des geschützten Speichers eines anderen Benutzers anzuzeigen, ein Benutzer, der eins dieser Tools versehendlich ausführt, könnte jedoch sein Passwort ungewollt einem Angreifer anzeigen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, Passwörter über die AutoVervollständigen-Funktion zu speichern.

Internetsystemsteuerung: Seite "Erweitert" deaktivieren

Wenn Sie diese Einstellung aktivieren, kann der Benutzer auf die Registerkarte *Erweitert* des Dialogfensters *Internetoptionen* nicht mehr zugreifen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die erweiterten Einstellungen zu verändern.

Internetsystemsteuerung: Seite "Sicherheit" deaktivieren

Diese Einstellung entfernt die Registerkarte *Sicherheit* aus dem Dialogfenster *Internetoptionen.*

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die Sicherheitseinstellungen zu verändern.

Offlineseiten: Entfernen von Channels deaktivieren

Diese Einstellung verhindert, dass Benutzer Channels entfernen. Channels sind Webseiten, die auf dem Computer nach einem Zeitplan automatisch von Channelprovider aktualisiert werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Es könnten ohne direkte Interaktion des Benutzers Daten an dessen Browser gesendet werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer können keine Channels entfernen.

Offlineseiten: Hinzufügen von Zeitplänen für Offlineseiten deaktivieren

Diese Einstellung verhindert, dass Benutzer Webseiten für eine Offlineanzeige definieren. Sie erzeugt durch das Herunterladen der Offlineinhalte Serverlast.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die Zeitpläne für Offlineseiten zu erstellen.

Offlineseiten: Alle geplanten Offlineseiten deaktivieren

Diese Einstellung deaktiviert bestehende Zeitpläne für Offlineseiten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**

- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die Zeitpläne für Offlineseiten anzuzeigen.

Offlineseiten: Channel-Benutzeroberfläche vollständig deaktivieren

Diese Einstellung verhindert, dass die Benutzer auf die Channeleinstellungen zugreifen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, auf die Channel-Benutzerschnittstelle zuzugreifen.

Offlineseiten: Download von abonnierten Siteinhalten deaktivieren

Diese Einstellung verhindert, dass Benutzer Inhalte von Webseiten herunterladen, die sie abonniert haben. Die Synchronisation mit diesen Webseiten findet jedoch trotzdem statt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**

- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, über Seitenabonnements Inhalte herunterzuladen.

Offlineseiten: Das Bearbeiten und Erstellen von geplanten Gruppen deaktivieren

Diese Einstellung verhindert, dass Benutzer Zeitpläne für die Offlinenutzung von Webseiten erstellen, ändern oder löschen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, Zeitpläne zu erstellen, zu ändern oder zu entfernen.

Offlineseiten: Bearbeiten von Zeitplänen für Offlineseiten deaktivieren

Diese Einstellung verhindert, dass Benutzer die bestehenden Zeitpläne verändern.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, Zeitpläne zu bearbeiten.

Offlineseiten: Trefferprotokollierung für Offlineseiten deaktivieren

Diese Einstellung verhindert, dass Channelprovider Informationen darüber erlangen, wann die Channelseiten von den Offlinebenutzern angezeigt wurden. Wenn die Einstellung aktiviert ist, deaktiviert sie alle Channel-Protokolleinstellungen die von Channelprovidern über das Channel Definition Format (.cdf) konfiguriert wurden. Die .cdf-Dateien legen den Zeitplan und andere Einstellungen für das Herunterladen von Webinhalten fest.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Die Trefferprotokolle werden für Benutzer, die ohne Verbindung auf Seiten zugreifen, nicht mehr an die entsprechenden Webseiten weitergeleitet.

Offlineseiten: Entfernen von Channels deaktivieren

Diese Einstellung verhindert, dass Benutzer die Channelsynchronisierung im Internet Explorer deaktivieren.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**

- **Nicht konfiguriert**

Anmerkung: Diese Richtlinie verhindert nicht, dass Benutzer aktive Inhalte vom Desktop entfernen.

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, Channels zu entfernen oder die Channelsynchronisation zu verhindern

Offlineseiten: Entfernen von Zeitplänen für Offlineseiten deaktivieren

Diese Einstellung verhindert, dass Benutzer die vorgegebenen Zeitpläne für die Offlineanzeige von Webseiten verändern oder löschen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die Zeitpläne für Offlineseiten zu entfernen.

Bildschirmschoner-Einstellungen

Bildschirmschoner wurden ursprünglich zum Schutz der Kathodenstrahlröhren von Monitoren entwickelt. Sie haben sich im Lauf der Zeit zu einem Sicherheitswerkzeug weiterentwickelt, indem sie den Bildschirm automatisch sperren, wenn der Benutzer seinen Arbeitsplatz verlässt und vergisst diesen zu sperren. Die Einstellungen für Bildschirmschoner können über den folgenden Pfad konfiguriert werden:

Benutzerkonfiguration\Administrative Vorlagen\Systemsteuerung\Anzeige

Kennwortschutz für den Bildschirmschoner verwenden

Diese Einstellung legt fest, ob der Bildschirmschoner durch ein Passwort geschützt ist. Ist sie aktiviert, dann ist das Kontrollkästchen **Passwortschutz** auf der Registerkarte *Bildschirmschoner* des Dialogfensters *Anzeigeeigenschaften* gesperrt. Der Passwortschutz ist dann aktiviert. Sie sollten zusätzlich die Einstellung **Bildschirmschoner Zeitlimit** konfigurieren.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Um die Registerkarte **Bildschirmschoner** vollständig zu entfernen, verwenden Sie die Einstellung **Registerkarte Bildschirmschoner entfernen**.

Sicherheitslücken

Wenn kein Passwortschutz für den Bildschirmschoner verwendet wird, und der Benutzer seinen Desktop nicht beim Verlassen des Arbeitsplatzes sperrt, dann ist die Arbeitsstation ungeschützt.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer müssen ihre Computer nach einem Start des Bildschirmschoners entsperren.

Bildschirmschoner

Diese Einstellung aktiviert den Bildschirmschoner. Wenn sie deaktiviert ist, wird kein Bildschirmschoner gestartet. Wenn die Einstellung aktiviert ist und die folgenden zwei Bedingungen zutreffen, dann wird der Bildschirmschoner verwendet: Im Feld **Bildschirmschoner** ist ein gültiger Bildschirmschoner angegeben, und im Feld **Wartezeit** ist ein Wert größer 0 angegeben.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Damit die oben beschriebenen Einstellungen verwendet werden können, muss diese Einstellung aktiviert sein.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Diese Einstellung aktiviert die Bildschirmschoner auf den Computern der Umgebung.

Programmname des Bildschirmschoners

Diese Einstellung definiert den Bildschirmschoner, der ausgeführt wird. Wenn die Einstellung aktiviert ist, kann der Benutzer auf die Auswahlliste im Feld **Bildschirmschoner** nicht mehr zugreifen. Geben Sie den vollständigen Dateinamen des Bildschirmschoners an, inklusive der Dateiendung .scr. Wenn er sich nicht im Ordner *%Systemroot%\System32* befindet, müssen Sie außerdem den vollqualifizierten Pfad der Datei angeben.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert** – mit dem Namen der Datei des Bildschirmschoners.
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Diese Einstellung kann durch die Einstellung **Bildschirmschoner** überschrieben werden. Wenn diese deaktiviert ist, wird kein Bildschirmschoner gestartet - unabhängig davon, ob hier eine Datei definiert ist.

Sicherheitslücken

Es muss ein gültiger Dateiname für einen Bildschirmschoner angegeben werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **scrnsave.scr** - dies ist der „Leerer Bildschirm“ Bildschirmschoner - oder einen Bildschirmschoner Ihrer Wahl.

Mögliche Auswirkungen

Der definierte Bildschirmschoner wird nach der konfigurierten Wartezeit ausgeführt.

Bildschirmschoner Zeitlimit

Diese Einstellung definiert, wie lange der Benutzer inaktiv sein muss, bevor der Bildschirmschoner gestartet wird. Der Wert kann zwischen 1 Sekunde und 86.000 Sekunden (24 Stunden) liegen. Die Einstellung hat unter den folgenden Bedingungen keine Auswirkungen:

- Sie ist deaktiviert oder nicht konfiguriert.
- Die Wartezeit ist auf 0 gesetzt.
- Die Einstellung **Kein Bildschirmschoner** ist Aktiviert.
- Es ist weder unter der Einstellung **Programmname des Bildschirmschoners**, noch im Feld **Bildschirmschoner** unter der Registerkarte **Bildschirmschoner** des Dialogfensters **Anzeigeeigenschaften** ein gültiger Bildschirmschoner angegeben.

Wenn die Einstellung nicht konfiguriert ist, wird die Wartezeit verwendet, die auf dem Client konfiguriert ist. Die Standardeinstellung ist hier 15 Minuten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert** – mit einem benutzerdefinierten Wert zwischen 0 und 86.000 Sekunden.
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Damit der Bildschirmschoner aktiv wird, muss eine gültige Wartezeit konfiguriert sein.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **600 Sekunden**.

Mögliche Auswirkungen

Nach fünf Minuten Inaktivität des Benutzers wird der Bildschirmschoner gestartet.

9

Administrative Vorlagen von Windows XP, Office XP und Windows Server 2003

Der Abschnitt administrative Vorlagen der Gruppenrichtlinie umfasst registrierungsbasierte Einstellung, die das Verhalten und das Erscheinungsbild der Computer Ihrer Umgebung bestimmen. Sie wirken sich außerdem auf das Verhalten von Betriebssystemkomponenten und Anwendungen aus. Es gibt bereits eine große Menge solcher Einstellung. Sie können durch das Importieren von .adm-Dateien weitere hinzufügen.

Dieses Kapitel beschreibt die unter dem Knoten *Computerkonfiguration* und dem Knoten *Benutzerkonfiguration* vorhandenen administrativen Vorlagen.

Es werden nur die Einstellung unter Microsoft® Windows® XP, Microsoft Office XP und Microsoft Windows Server 2003 besprochen, die für die Absicherung von Computern relevant sind. Die nicht besprochenen Einstellungen beziehen sich unter anderem auf Microsoft NetMeeting®, Anwendungskompatibilität, Taskplaner, Windows Installer, Windows Messenger und den Windows Media® Player.

Internet Explorer Einstellung

Der Microsoft Internet Explorer ist der in Windows XP und Windows Server 2003 enthaltene Webbrowser. Sie können viele seiner Features über die Gruppenrichtlinien verwalten. Sie finden die entsprechenden Einstellungen unter:
Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Internet Explorer

Automatische Installation von Internet Explorer-Komponenten deaktivieren

Die Aktivierung dieser Einstellung verhindert, dass der Internet Explorer Komponenten herunterlädt, wenn der Benutzer Webseiten aufruft, für die diese erforderlich wären. Wenn die Einstellung deaktiviert oder nicht konfiguriert ist, wird der Benutzer jedes Mal zur Installation der Komponenten aufgefordert. Über diese Richtlinie kann der Administrator kontrollieren, welche Komponenten vom Benutzer installiert werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Böswillige Webseitenbetreiber können Komponenten installieren, die schädlichen Programmcode ausführen. Dies könnte zur ungewollten Verbreitung von Daten, zum Verlust von Daten oder zur Instabilität des Systems führen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Der Internet Explorer ist nicht mehr in der Lage, die für Webseiten benötigten Komponenten automatisch herunterzuladen.

Periodische Überprüfungen auf Softwareaktualisierungen von Internet Explorer deaktivieren

Wenn die Einstellung aktiviert ist, wird verhindert, dass der Internet Explorer nach neuen Versionen des Browsers sucht und den Benutzer darüber informiert. Wenn sie deaktiviert oder nicht konfiguriert ist, sucht der Internet Explorer alle **30 Tage** nach neuen Versionen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Obwohl Microsoft alle Patches und Servicepacks vor deren Veröffentlichung ausführlich testet, möchten manche Organisationen möglicherweise eine genauere Kontrolle über die auf ihren Systemen installierten Updates behalten. Wenn die Einstellung aktiviert ist, werden keine Updates für den Internet Explorer heruntergeladen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Der Internet Explorer ist nicht mehr in der Lage, Hotfixes und Servicepacks automatisch herunterzuladen. Daher muss hierfür vom Administrator ein anderes Verfahren implementiert werden.

Anzeigen des Begrüßungsbildschirms deaktivieren

Wenn dieser Einstellung aktiviert ist, wird der Begrüßungsbildschirm – er zeigt Programmname, Lizenz und Copyright-Informationen an - beim Start des Browsers nicht mehr angezeigt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

In einigen Organisationen ist es möglicherweise nicht gewollt, dass den Benutzern die Lizenz und die Version des Internet Explorers bekannt sind.

Gegenmaßnahmen

Setzten Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Der Internet Explorer startet schneller, wenn er keinen Begrüßungsbildschirm anzeigt.

Deaktivieren von Software-Update Shell-Benachrichtigungen beim Programmstart

Diese Einstellung definiert, ob Programme, die den Microsoft Software Distribution Channel verwenden, den Benutzer bei der Installation neuer Komponenten benachrichtigen. Der Software Distribution Channel ist ein dynamisches Softwareupdate über die Open Software Distribution (OSD)-Technologie. Wenn die Einstellung aktiviert ist, werden die Benutzer nicht benachrichtigt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Organisationen, die OSD-Werkzeuge und -Technologien verwenden, möchten möglicherweise, dass die Benutzer bei einer Installation von Patches und Servicepacks auf ihren Systemen nicht benachrichtigt werden. Diese könnten versuchen den Installationsprozess abzubrechen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**

Mögliche Auswirkungen

Benutzer werden bei Updates über OSD-Technologien nicht benachrichtigt.

Proxy-Einstellung pro Computer vornehmen (anstelle von pro Benutzer)

Wenn diese Einstellung aktiviert ist, können die Benutzer keine eigenen Proxy-Einstellungen mehr vornehmen. Sie müssen die Einstellungen verwenden, die für alle Benutzer dieses Computers gelten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn die Einstellung deaktiviert oder nicht konfiguriert ist, können die Benutzer ihre eigenen Proxy-Einstellungen verwenden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Alle Benutzer werden dazu gezwungen, die für den Computer definierten Proxy-Einstellungen zu verwenden.

Sicherheitszonen: Benutzer können Sites nicht hinzufügen oder entfernen

Wenn dieser Einstellung aktiviert ist, ist das Hinzufügen oder Entfernen von Webseiten zu Sicherheitszonen nicht mehr möglich.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Aktivieren Sie alternativ die Einstellung **Sicherheitsseite deaktivieren**, unter *Benutzerkonfiguration\Administrative Vorlagen\Windows Komponenten\Internet Explorer\Internetoptionen*. Sie entfernt die gesamte Registerkarte Sicherheit.

Sicherheitslücken

Wenn die Einstellung nicht konfiguriert ist, ist es den Benutzern möglich die Zoneneinstellungen zu verändern. Sie könnten so auf gefährliche Webseiten zugreifen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Diese Richtlinie verhindert, dass Benutzer die Einstellungen der Sicherheitszonen verändern, die der Administrator vorgenommen hat. Dies kann nur noch der Administrator.

Sicherheitszonen: Benutzer können Einstellung nicht ändern

Die Aktivierung dieser Einstellung bewirkt, dass der Schalter **Stufe anpassen** und der Schieberegler **Sicherheitslevel dieser Zone** auf der Registerkarte **Sicherheit** der **Internetoptionen** nicht mehr zu Verfügung stehen. Wenn die Einstellung deaktiviert oder nicht konfiguriert ist, kann der Benutzer die Sicherheitsoptionen ändern.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Aktivieren Sie alternativ die Einstellung **Sicherheitsseite deaktivieren**, unter *Benutzerkonfiguration\Administrative Vorlagen\Windows Komponenten\Internet Explorer\Internetoptionen*. Sie entfernt die gesamte Registerkarte Sicherheit.

Sicherheitslücken

Wenn die Einstellung nicht konfiguriert ist, ist es den Benutzern möglich die Zoneneinstellungen zu verändern. Sie könnten so auf gefährliche Webseiten zugreifen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Diese Richtlinie verhindert, dass Benutzer die Einstellungen der Sicherheitszonen verändern, die der Administrator vorgenommen hat. Dies kann nur noch der Administrator.

Sicherheitszonen: Die Einstellung für Sicherheitszonen statisch festlegen

Wenn die Einstellung aktiviert ist, werden die Einstellungen, die ein Benutzer vornimmt für alle Benutzer des Computers verwendet. Wenn sie deaktiviert oder nicht konfiguriert ist, verwenden alle Benutzer ihre eigenen Einstellungen für die Sicherheitszonen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn die Einstellung nicht konfiguriert ist, ist es den Benutzern möglich die Zoneneinstellungen zu verändern. Sie könnten so auf gefährliche Webseiten zugreifen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Diese Richtlinie verhindert, dass Benutzer die Einstellungen der Sicherheitszonen verändern.

Terminalserver-Richtlinien konfigurieren

Die Terminaldienste-Komponente von Windows Server 2003 baut auf der soliden Grundlage des Anwendungsserver-Modus der Windows 2000 Terminaldienste auf. Sie stellt nun auch die neuen Möglichkeiten der Windows XP Terminaldienste zur Verfügung. Die Terminaldienste von Windows Server 2003 können die Softwareverteilung eines Unternehmens über eine Vielzahl von Szenarios verbessern. Wenn ein Benutzer eine Anwendung auf einem Terminalserver startet, wir diese auf dem Terminalserver ausgeführt. Nur die Informationen im Bezug auf Tastatur, Maus und Anzeige werden über das Netzwerk übertragen. Jeder Benutzer hat seine eigene Sitzung. Diese wird vom Serverbetriebssystem verwaltet und ist von allen anderen Sitzungen vollständig unabhängig. Sie können die Richtlinieneinstellungen für Terminalserver über den folgenden Pfad konfigurieren: *Computerkonfiguration\Administrative Vorlagen\Windows Komponenten\Terminaldienste*

Abmelden von Administratoren in Konsolensitzung verweigern

Dieser Einstellung definiert, ob es einem Administrator gestattet ist, eine Verbindung zur Konsole eines Servers aufzubauen und damit den momentan an der Konsole angemeldeten Administrator abzumelden. Die Konsolensitzung wird auch Sitzung 0 genannt. Ein Konsolenzugriff kann über den Schalter /console im Feld Computername einer Remotedesktopverbindung, oder über die Eingabeaufforderung durchgeführt werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Wenn diese Einstellung **aktiviert** ist, wird verhindert, dass ein am System angemeldeter Administrator abgemeldet wird und so möglicherweise Daten verloren gehen. Bei den Einstellungen deaktiviert und nicht konfiguriert ist dies möglich.

Sicherheitslücken

Ein Angreifer, der es geschafft hat eine Terminalserver-Sitzung aufzubauen und administrative Privilegien zu erlangen, könnte es dem legalen Administrator sehr schwer machen, die Kontrolle über den Computer über die Sitzung 0 zurückzuerlangen. Wenn ein Angreifer einen solchen Zugriff auf einen Computer erlangt hat, hat dieser allerdings den Computer bereits vollständig übernommen. Daher ist der Wert eventueller Gegenmaßnahmen ehr gering.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Ein Administrator ist nicht in der Lage, andere Administratoren von der Sitzung 0 Konsole abzumelden.

Anpassen der Berechtigungen durch lokale Administratoren nicht zulassen

Diese Einstellung definiert, ob ein Administrator die Sicherheitsberichtigungen im Terminaldienste-Konfigurationstool ändern kann. So können Sie verhindern, dass die Sicherheitsbeschreibungen der Benutzergruppen auf der Registerkarte Berechtigungen geändert werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Die Standardmethode zur Verwaltung des Benutzerzugriffs ist das Hinzufügen der Benutzer zur Gruppe **Remotedesktop-Benutzer**.

Sicherheitslücken

Ein Angreifer, der administrativen Zugriff auf einen Server, der die Terminaldienste ausführt, erlangt hat, kann die Berechtigung ändern und so die Benutzer daran hindern eine Verbindung zum Server aufzubauen. Dies stellt einen DoS-Zustand dar. Wenn ein Angreifer einen solchen Zugriff auf einen Computer erlangt hat, hat dieser allerdings den Computer bereits vollständig übernommen. Daher ist der Wert eventueller Gegenmaßnahmen ehr gering.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Die Sicherheitsbeschreibungen können über die Registerkarte Berechtigungen nicht geändert werden.

Regeln für Remoteüberwachung von Terminaldienste-Benutzersitzungen festlegen

Diese Einstellung legt die Remoteüberwachung fest, die in einer Terminalsitzung gestattet ist. Eine Remoteüberwachung kann mit oder ohne Erlaubnis des Benutzers durchgeführt werden. Über diese Einstellung können Sie zwei unterschiedliche Varianten der Remoteüberwachung konfigurieren: **Sitzung anzeigen** erlaubt die Remoteüberwachung einer Sitzung. **Vollzugriff** erlaubt mit der Sitzung zu interagieren. Wenn die Einstellung aktiviert ist, ist es den Administratoren möglich, in die Terminalsitzung eines Benutzers einzugreifen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Keine Remoteüberwachung erlaubt**
  - **Vollzugriff mit Erlaubnis des Benutzers**
  - **Vollzugriff ohne Erlaubnis des Benutzers**
  - **Sitzung anzeigen mit Erlaubnis des Benutzers**
  - **Sitzung anzeigen ohne Erlaubnis des Benutzers**
- **Deaktiviert**

- **Nicht konfiguriert**

Anmerkung: Diese Einstellung gibt es unter *Computerkonfiguration* und unter *Benutzerkonfiguration*. Wenn beide konfiguriert sind, hat die Einstellung unter *Computerkonfiguration* Vorrang.

Sicherheitslücken

Ein Angreifer, der administrative Privilegien auf einem Server erlangt hat, könnte das Remoteüberwachungs-Feature ausnutzen, um die Aktivitäten von Benutzern zu verfolgen. Dies könnte zum Verlust vertraulicher Informationen führen. Der Wert möglicher Gegenmaßnahmen ist allerdings gering, da ein Angreifer, der administrative Rechte erlangt hat, die vollständige Kontrolle über den Computer übernommen hat.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** und **Keine Remoteüberwachung erlaubt**.

Mögliche Auswirkungen

Administratoren sind nicht in der Lage, die Remoteüberwachung zu verwenden. Sie können Terminalserver-Benutzern keine Unterstützung bieten.

Die Datenumleitungs-Einstellungen können Sie über den folgenden Pfad konfigurieren: *Computerkonfiguration\Administrative Vorlagen\Windows Komponenten\Terminaldienste\Client/Server-Datenumleitung*

Zeitzonenumleitung zulassen

Diese Einstellung definiert, ob es dem Clientcomputer gestattet ist, seine Zeitzoneneinstellungen auf die Terminalserver-Sitzung umzuleiten. Als Standard ist die Einstellung deaktiviert. Die Zeitzone der Sitzung ist somit dieselbe, wie die des Terminalservers. Der Client kann seine Zeitzone nicht umleiten. Im Moment ist eine Umleitung nur über eine Remotedesktopverbindung oder mit Windows CE 5.1 möglich. Die Konsolensitzung verwendet immer die Einstellungen des Servers. Wenn die Einstellung vom Administrator geändert wird, betrifft dies nur neue Sitzungen. Bestehende Sitzungen werden nicht beeinflusst.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Eine Zeitzonenumleitung ist nur mit einem Windows Terminalserver möglich.

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Deaktiviert**.

Mögliche Auswirkungen

Eine Zeitzonenumleitung ist nicht möglich.

Zwischenablageumleitung nicht zulassen

Diese Einstellung legt fest, ob die Umleitung der Zwischenablage gestattet ist. Als Standard ist sie deaktiviert. Dies ermöglicht die Umleitung der Zwischenablage.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Eine Umleitung der Zwischenablage ist nicht möglich.

Audioumleitung zulassen

Diese Einstellung legt fest, ob der Benutzer die Audioausgaben der Terminalsitzung auf dem lokalen Computer abspielen kann. Als Standard ist sie deaktiviert. Dies gestattet den Benutzern nicht die Audioausgaben umzuleiten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Eine Umleitung der Audioausgaben ist nicht möglich.

COM-Anschlussumleitung nicht zulassen

Dieser Einstellung legt fest, ob die Umleitung von Daten an die COM-Ports des Clients in der Terminalsitzung möglich ist. Als Standard ist die Einstellung deaktiviert. Dies verhindert, dass Serverdaten auf lokale COM-Ports umgeleitet werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Eine Umleitung der COM-Ports ist nicht möglich.

Clientdruckerumleitung nicht zulassen

Diese Einstellung legt fest, ob die Umleitung von Druckern des Clients an die Terminalsitzung möglich ist. Als Standard ist die Einstellung deaktiviert. Dies ermöglicht, dass lokale Drucker umgeleitet werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Eine Umleitung der Drucker ist nicht möglich.

LPT-Anschlussumleitung nicht zulassen

Diese Einstellung legt fest, ob die Umleitung von LPT-Anschlüssen des Clients an die Terminalsitzung möglich ist. Als Standard ist die Einstellung deaktiviert. Dies ermöglicht, dass die LPT-Anschlüsse umgeleitet werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Eine Umleitung der LPT-Anschlüsse ist nicht möglich.

Laufwerkumleitung nicht zulassen

Als Standard werden die Clientlaufwerke automatisch bei einer Verbindung gemappt. Sie tauchen in der Ordernstruktur der Sitzung im Windows Explorer unter dem Format <*Laufwerksbuchstabe*> auf <C*omputername*> auf. Wenn Sie die Einstellung aktivieren, wird dies verhindert.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Eine Umleitung der Laufwerke ist nicht möglich.

Standardclientdrucker nicht als Standarddrucker in einer Sitzung festlegen

Über diese Einstellung kann verhindert werden, dass der lokale Standarddrucker der Standarddrucker der Terminalsitzung wird. Als Standard ist diese Einstellung deaktiviert. Damit ist der Standarddrucker der gleiche, wie der des lokalen Clients.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Über die Terminalsitzung könnten ohne Interaktion des Benutzers Daten an dessen Computer übertragen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **aktiviert**.

Mögliche Auswirkungen

Der Standarddrucker des Clients wird nicht der Standarddrucker der Terminalsitzung.

Die Verschlüsselungs- und Sitzungseinstellungen können Sie über den folgenden Pfad festlegen:
Computerkonfiguration\Administrative Vorlagen\Windows Komponenten\Terminaldienste\Verschlüsselung und Sicherheit

Verschlüsselungsstufe der Clientverbindung festlegen

Diese Einstellung legt fest, ob eine Verschlüsselung für eine Terminalsitzung durchgesetzt wird. Wenn sie aktiviert ist, können Sie eine Verschlüsselungsstufe festlegen. Die Standardeinstellung ist **Hohe Verschlüsselung**.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Kompatibel:** Die Sitzung wird in beide Richtungen mit dem stärksten vom Client unterstützten Schlüssel verschlüsselt. Verwenden Sie die Option, wenn in der Umgebung ältere Clients vorhanden sind.
  - **Hohe Verschlüsselung:** Die Sitzung wird in beide Richtung mit einem 128-Bit Schlüssel verschlüsselt. Verwenden Sie die Option, wenn in Ihrer Umgebung nur 128-Bit Clients vorhanden sind. Zum Beispiel Remotedesktopverbindungs-Clients. Clients, die eine solche Verschlüsselung nicht unterstützen, können keine Verbindung aufbauen.
  - **Geringe Verschlüsselung**: Nur die Daten, die vom Client zum Server gesendet werden, werden mit einem 56-Bit Schlüssel verschlüsselt. Die Daten vom Server zum Client werden nicht verschlüsselt.
- **Deaktiviert**
- **Nicht konfiguriert**

Wichtig: Wenn die Einstellung Systemkryptografie: **FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden** aktiviert wurde, können Sie über die Einstellung **Verschlüsselungsstufe der Clientverbindung festlegen** die Verschlüsselungsstufe nicht ändern.

Sicherheitslücken

Wenn es den Clients möglich ist, eine Sitzung mit geringer Verschlüsselung aufzubauen, hat ein Angreifer eine bessere Chance den Netzwerkverkehr zu entschlüsseln.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Hohe Verschlüsselung**.

Mögliche Auswirkungen

Clients, die eine 128-Bit Verschlüsselung nicht unterstützen, können keine Terminalsitzung aufbauen.

Clients bei der Verbindungsherstellung immer zur Kennworteingabe auffordern

Wenn diese Einstellung aktiviert ist, muss der Benutzer bei jeder Verbindung ein Passwort eingeben – auch wenn dieser bereits im Remotedesktop-Client ein Passwort angegeben hat.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzername und Passwort können beide vom Benutzer im Remotedesktop-Client gespeichert werden. Wenn ein Angreifer dann auf diesen Client Zugriff erlangt hat, und eine erneute Eingabe des Passwortes bei einer Verbindung nicht erzwungen wird, hat der Angreifer die Möglichkeit eine Terminalsitzung aufzubauen – auch wenn er das Passwort des Benutzers tatsächlich gar nicht kennt.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Die Benutzer müssen bei jeder neuen Terminalsitzung ein Passwort angeben.

Sie können Sie RPC-Sicherheitseinstellung für Terminalserver über den folgenden Pfad konfigurieren: *Computerkonfiguration\Administrative Vorlagen\Windows Komponenten\Terminaldienste\Verschlüsselung und Sicherheit\RPC Sicherheit*

Sicherer Server (Sicherheit erforderlich)

Wenn diese Einstellung aktiviert ist, legt dies fest, dass der Terminalserver eine sichere Remote Procedure Call (RPC)-Kommunikation mit den Clients erfordert. Wenn sie deaktiviert ist, fordert der Terminalserver zwar immer eine sichere Kommunikation an, akzeptiert jedoch auch eine ungesicherte Kommunikation.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Verwenden Sie für die Administration und Konfiguration der Terminaldienste die RPC-Schnittstelle.

Sicherheitslücken

Wenn eine ungesicherte RPC-Kommunikation möglich ist, wird der Server für Man-in-the-middle-Angriffe verwundbar. Ein Man-in-the-middle-Angriff findet statt, wenn ein Eindringling Pakete zwischen Client und Server abfängt, und diese vor deren Weiterleitung verändert. Meist wird versucht, über diese Änderungen den Client oder den Server zur Bekanntgabe von sensiblen Informationen zu bringen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Clients, die sicheres RPC nicht unterstützen, sind nicht in der Lage den Server remote zu verwalten.

Die RPC-Sicherheitseinstellungen für Terminalserver können Sie über den folgenden Pfad festlegen: *Computerkonfiguration\Administrative Vorlagen\Windows Komponenten\Terminaldienste\Verschlüsselung und Sicherheit\RPC Sicherheit\Sitzungen*

Zeitlimit für getrennte Sitzungen festlegen

Diese Einstellung legt fest, wie lange eine getrennte Sitzung auf dem Server aktiv bleibt. Als Standard ist es Benutzern möglich, eine Terminalsitzung ohne Abmeldung zu beenden. In diesem Status werden die Programme in der Sitzung weiter ausgeführt, auch wenn der Benutzer nicht mehr verbunden ist. Normalerweise werden diese Sitzungen ohne Zeitlimit weitergeführt. Wenn die Einstellung aktiviert ist, werden sie nach einer bestimmten Zeit getrennt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Nie**
  - **1 Minute**
  - **5 Minuten**
  - **10 Minuten**
  - **15 Minuten**
  - **30 Minuten**
  - **1 Stunde**
  - **2 Stunden**
  - **3 Stunden**
  - **1 Tag**
  - **2 Tage**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Diese Einstellung wirkt sich auf Konsolensitzungen, wie zum Beispiel Remotedesktopverbindungen, nicht aus. Sie steht unter *Computerkonfiguration* und unter *Benutzerkonfiguration* zur Verfügung. Wenn beide konfiguriert sind, hat die Einstellung unter *Computerkonfiguration* Vorrang.

Sicherheitslücken

Jede Terminalserver-Sitzung verbraucht Systemressourcen. Wenn getrennte Sitzungen nicht nach einer bestimmten Zeit beendet werden, könnten dem Server die Ressourcen ausgehen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** und **1 Tag**.

Mögliche Auswirkungen

Sitzungen von Benutzern, die vergessen sich abzumelden, werden nach 24 Stunden Inaktivität beendet.

Erneute Verbindung nur vom ursprünglichen Client zulassen

Wenn diese Einstellung aktiviert ist, wird verhindert, dass Benutzer eine neue Verbindung zu einer

bestehenden Sitzung über einen anderen Client aufbauen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Wichtig: Diese Einstellung wird nur für Citrix ICA Clients unterstützt, die bei einer Verbindung eine Seriennummer zur Verfügung stellen. Wenn Benutzer eine Verbindung über einen Windows-Client aufbauen, wird sie ignoriert. Sie steht unter *Computerkonfiguration* und unter *Benutzerkonfiguration* zur Verfügung. Wenn beide konfiguriert sind, hat die Einstellung unter *Computerkonfiguration* Vorrang.

Sicherheitslücken

Normalerweise können Benutzer eine Terminalsitzung von jedem Computer aus fortsetzen. Diese Einstellung verhindert das. Ihr Wert ist eher gering, da sie nur für Benutzer von Citrix ICA Clients durchgesetzt wird.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer, die eine Verbindung über Citrix ICA Clients aufbauen, können eine bestehende Sitzung nur von dem Client aus weiterführen, von dem aus diese aufgebaut wurde.

Internetinformationsdienste

IIS 6.0 (Internet Information Services), der von Windows Server 2003 zur Verfügung gestellte Webserver, ermöglicht eine einfache Veröffentlichung von Dokumenten und Informationen im Intranet und Internet. Sie können die IIS-Einstellung über den folgenden Pfad konfigurieren: *Computerkonfiguration\Administrative Vorlagen\Windows Komponenten\Internetinformationsdienste*

IIS-Installation verhindern

Die IIS 6.0 sind als Standard unter Windows Server 2003 nicht installiert. Wenn die Einstellung aktiviert ist, können sie auch später nicht installiert werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

In den vorhergehenden Versionen der IIS und den von ihnen abhängigen Anwendungen gab es einige Sicherheitslöcher. Obwohl die IIS 6.0 sicherer als ihre Vorgänger sind, ist es natürlich möglich, dass es bis jetzt unentdeckte Sicherheitslöcher gibt. Daher möchten Organisationen möglicherweise

sicherstellen, dass diese auf Nicht-Webservern nicht installiert werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Sie sind nicht in der Lage, Windows Komponenten oder Anwendungen zu installieren, die die IIS benötigen. Es wird bei einem solchen Versuch keine Fehlermeldung angezeigt. Wenn die IIS bereits installiert sind, hat diese Einstellung keine Auswirkungen.

Windows Update

Windows Update wird für das Herunterladen von Security-Fixes, kritischen Updates und den aktuellsten Hilfedateien, Treibern und Internetprodukten verwendet. Sie können Windows Update über den folgenden Pfad konfigurieren:
Computerkonfiguration\Administrative Vorlagen\Windows Komponenten\Windows Update

Automatische Updates konfigurieren

Wenn diese Einstellung aktiviert ist, verwenden die Computer Ihrer Umgebung automatische Updates. Wenn sie deaktiviert ist, müssen Sie die verfügbaren Updates manuell von der Windows Update Webseite unter http://windowsupdate.microsoft.com herunterladen. Administratoren können die automatischen Updates allerdings weiterhin über die Systemsteuerung konfigurieren.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **2: Vor dem Herunterladen und dem Installieren von Updates benachrichtigen.**
  - **3: Updates automatisch herunterladen und vor der Installation benachrichtigen.** Dies ist die Standardeinstellung.
  - **4: Updates automatisch herunterladen und diese nach dem definierten Zeitplan installieren.** Wenn kein Zeitplan konfiguriert ist, wird die Installation täglich um 3:00 Uhr nachts durchgeführt. Wenn für die Fertigstellung der Installation Neustarts erforderlich sind, werden diese automatisch durchgeführt. Sollte ein Benutzer angemeldet sein, wird dieser benachrichtigt und kann den Neustart verzögern.
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn das automatische Update aktiviert ist, verfügen die Computer ihrer Organisation immer über die neusten Updates und Servicepacks. So werden Sicherheitslücken schnellstmöglich geschlossen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** und wählen Sie die Option **4 = Updates automatische herunterladen und diese nach dem definierten Zeitplan installieren**.

Mögliche Auswirkungen

Kritische Betriebssystemupdates und Servicepacks werden automatisch heruntergeladen und täglich um 3:00 Uhr nachts installiert.

Kein automatischer Neustart für geplante Installationen automatischer Updates

Wenn die Einstellung aktiviert ist, wird kein automatischer Neustart nach der Installation von Updates ausgeführt – auch dann nicht, wenn ein Benutzer angemeldet ist. Stattdessen benachrichtigt das automatische Update den Benutzer darüber, dass er den Computer neu starten muss um die Installation abzuschließen. Bedenken Sie, dass weitere Updates erst nach dem Neustart erkannt und installiert werden. Wenn die Einstellung deaktiviert ist, wird der Computer nach der Benachrichtigung des Benutzers nach 5 Minuten neu gestartet.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Dieser Einstellung ist nur wirksam, wenn die Einstellung **Automatische Updates konfigurieren** für eine geplante Installation konfiguriert ist.

Sicherheitslücken

Manchmal muss für die Fertigstellung von Updates das Betriebssystem neu gestartet werden. Wenn dies nicht durchgeführt wird, ist das aktuelle Update nicht vollständig installiert, und neue Updates werden nicht erkannt und installiert.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Deaktiviert**.

Mögliche Auswirkungen

Es gibt einen ernsten Nachteil bei der Aktivierung dieser Einstellung. Ein automatischer Neustart wird auch auf den Servern durchgeführt. Bei kritischen Servern kann das zu einem unerwarteten temporären DoS-Zustand führen.

Geplante Installationen automatischer Updates erneut planen

Diese Einstellung legt den Zeitraum fest, den das automatische Update nach dem Systemstart wartet, bevor eine fehlgeschlagene Installation erneut durchgeführt wird. Wenn sie aktiviert ist, wird die Installation nach dem konfigurierten Zeitraum erneut durchgeführt. Ist sie deaktiviert, wird diese erst mit der nächsten geplanten Installation durchgeführt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert:** Ein benutzerdefinierter Wert zwischen **1** und **60** Minuten.
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Dieser Einstellung wirkt sich nur aus, wenn die Einstellung **Automatische Updates konfigurieren** für die geplante Installation konfiguriert ist. Ansonsten hat sie keinen Effekt.

Sicherheitslücken

Wenn nicht vor der nächsten Installation ein paar Minuten abgewartet wird, könnte dieses zu Konflikten mit beim Systemstart noch nicht vollständig gestarteten Anwendungen und Diensten führen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** und **10 Minuten**.

Mögliche Auswirkungen

Automatische Updates werden erst 10 Minuten nach dem Neustart des Computers durchgeführt.

Internen Pfad für den Microsoft Updatedienst angeben

Wenn dieser Einstellung aktiviert ist, legt sie einen Intranet-Server fest, der Updates der Microsoft Update Webseite zur Verfügung stellt. Dieser wird dann, anstelle der Microsoft Update Webseite, von den Computern Ihres Netzwerkes auf verfügbare Updates abgefragt. Damit Sie diese Einstellung verwenden können, müssen Sie zwei Servernamen angeben: Den Server, von dem die Update-Clients ihre Updates abfragen und erhalten, und den Server auf den die aktualisierten Uploadstatistiken der Arbeitsstationen hochgeladen werden. Sie können den gleichen Server für beide Funktionen verwenden. Auf diese Weise müssen Updateverbindungen nicht über eine Firewall aufgebaut werden, und Sie haben die Möglichkeit, die Updates vor deren Bereitstellung zu testen.

Die möglichen Werte für diese Einstellung sind:^

- **Aktiviert:** Wenn Sie dieser Einstellung verwenden, definieren Sie im Dialogfenster **Eigenschaften** die Namen des Updateservers und des Statistikservers.
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Wenn die Einstellung **Automatische Updates konfigurieren** deaktiviert ist, hat diese Einstellung keine Auswirkungen.

Sicherheitslücken

Einige Organisationen möchten Updates möglicherweise vor einer Bereitstellung testen. Außerdem wird der Verkehr auf den Firewalls, Routern und Proxy-Servern verringert, da die Updates nun nicht mehr von der Microsoft Webseite, sondern von dem internen SUS-Server (Software Update Services) heruntergeladen werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**. Geben Sie dann die entsprechenden Servernamen an.

Mögliche Auswirkungen

Kritische Updates und Servicepacks werden von den IT-Mitarbeitern der Organisation verwaltet.

Anmeldeeinstellungen

Diese Einstellungen beeinflussen die Anmeldung der Benutzer. Sie können sie unter dem folgenden Pfad konfigurieren:
Computerkonfiguration\Administrative Vorlagen\System\Anmeldung

Willkommenseite für "Erste Schritte" bei der Anmeldung nicht anzeigen

Diese Einstellung verhindert die Anzeige des Willkommensbildschirms von Microsoft Windows® 2000 Professional und Windows XP Professional. Sie betrifft nur Windows 2000 Professional und Windows XP Professional.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Diese Einstellung steht sowohl unter *Computerkonfiguration*, als auch unter *Benutzerkonfiguration* zur Verfügung. Wenn beide konfiguriert sind, hat die Einstellung unter *Computerkonfiguration* Vorrang.

Sicherheitslücken

Der Willkommensbildschirm ermöglicht es dem Benutzer den Windows XP Desktop kennen zu lernen. Einige Organisationen möchten dies möglicherweise nicht, da sie dem Benutzer andere Möglichkeiten der Schulung bieten.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Der Willkommensbildschirm wir den Benutzern nicht angezeigt.

Microsoft Office XP Custom Maintenance Wizard

Der Microsoft Office XP Custom Maintenance Wizard (Microsoft Office XP Anpassungsassistent) ermöglicht es Ihnen, die auf den Benutzercomputern installierten Features von Softwareprodukten zu aktualisieren. Der Assistent liest als erstes das Windows Installer Paket (.msi Datei) und erstellt dann eine neue Produktkonfigurationsdatei (.cmw). Danach verwendet er die .cmw-Datei, um die installierten Features auf den Computern der Benutzer zu aktualisieren.

Die administrativen Vorlagen (.adm) für Office XP sind unter Windows XP oder Windows Server 2003 normalerweise nicht vorhanden. Sie sind in den Office XP Resource Kit Tools enthalten. Diese können Sie unter http://www.microsoft.com/office/ork/xp/appndx/appa18.htm (englischsprachig) herunterladen. Nach der Installation der Tools finden Sie im Ordner %systemroot%\inf die folgenden Vorlagen:

- Access10.adm enthält die Einstellungen für Access 2002.
- Excel0.adm enthält die Einstellungen für Excel 2002.
- FP10.adm enthält die Einstellungen für Microsoft Front Page® 2002.
- GAL.adm enthält die Einstellungen für die Office XP Zwischenablage.
- Instlr11.adm enthält die Einstellungen für den Windows Installer.
- Office10.adm Einstellungen die für alle Office XP Anwendungen gelten.
- Outlk10.adm enthält die Einstellungen für Microsoft Outlook® 2002.
- Ppt10.adm enthält die Einstellungen für Microsoft PowerPoint® 2002.
- Pub10.adm enthält die Einstellungen für Publisher 2002.
- Word10.adm, enthält die Einstellungen für Word 2002.

► Um die .adm-Vorlagen im Snap-In Gruppenrichtlinie zu importieren

4. Klicken Sie mit der rechten Maustaste auf **Administrative Vorlagen** und dann auf **Administrative Vorlage hinzufügen/entfernen**.
5. Klicken Sie auf **Hinzufügen**
6. Wählen Sie die entsprechende .adm-Vorlage aus.

Die neuen Richtlinien werden in den entsprechenden Pfaden der Gruppenrichtlinie angezeigt.

Die Einstellungen des **Microsoft Office XP Custom Maintenance Wizard** können Sie unter dem folgenden Pfad konfigurieren:
Computerkonfiguration\Administrative Vorlagen\Microsoft Office XP\Custom Maintenance Wizard

Anwendung aller CMW-Dateien erlauben

Wenn der Benutzer nicht Administrator des Computers ist, müssen die CMW-Dateien in den CMW-Ordner, der durch die Sourcelist der Windows Installers definierten Installationsquelle der Anwendung, platziert werden. Über diese Einstellung können Sie dieses Verhalten ändern.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Ein böswilliger Benutzer, der seinen eigenen CMW-Ordner anpassen kann, könnte nicht autorisierte Softwarepakete auf dem Computer installieren.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Benutzer können nur aus den Quellen installieren, die in der Office XP Sourcelist des Windows

Installer definiert sind.

Microsoft Office XP Sicherheitseinstellungen

Microsoft Office XP umfasste einige Sicherheitsfeatures, die für eine starke Sicherheit bei gleichzeitiger Flexibilität sorgen. Sie können die Microsoft Office XP Sicherheitseinstellungen über den folgenden Pfad konfigurieren:
Computerkonfiguration\Administrative Vorlagen\Microsoft Office XP\ Security Settings

Access: Allen installierten Add-ins und Vorlagen vertrauen

Unter Microsoft Access wird diese Einstellung nur für COM Add-ins verwendet.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Sie haben die Möglichkeit allen momentan installierten Add-Ins und Vorlagen zu vertrauen. Damit wird allen mit Microsoft Office installierten Dateien vertraut - unabhängig davon, ob diese signiert sind oder nicht. Es ist möglich, dass ein Angriff über einen Virus, ein Trojanisches Pferd oder anderen feindlichen Code eingebettet in ein Office-Dokument, stattfindet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Es gibt keinen direkten Weg, im Voraus eine Liste von vertrauenswürdigen Quellen zu laden. Sie müssen jedes Zertifikat erst auf einem Testcomputer akzeptieren. Dies kann viel Zeit in Anspruch nehmen.

VBA für Office-Anwendungen deaktivieren

Diese Einstellung verhindert, das Excel, FrontPage, Outlook, PowerPoint, Microsoft Publisher und Word Microsoft Visual Basic® for Applications (VBA) verwenden. Durch diese Einstellung werden keine VBA-Dateien auf dem Computer installiert oder entfernt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

VBA wird von einigen Administratoren als Sicherheitsrisiko betrachtet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

VBA steht nicht zur Verfügung. Daher können Makros, Scripts und andere Anwendungen, die von VBA abhängig sind, fehlschlagen.

Excel: Makro-Sicherheitsebene

Über diese Einstellung können Sie den Makrovirusschutz konfigurieren.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Hoch**
    - **Unsignierte Makros**: Makros sind automatisch deaktiviert, und die Datei wird geöffnet.
    - **Signierte Makros:** Die Quelle und die Signatur des Makros legen fest, wie dieses gehandhabt wird.
    - **Vertrauenswürdige Quelle:** Signatur ist gültig: Makros sind automatisch aktiviert und die Datei wird geöffnet.
    - **Unbekannter Autor:** Signatur ist gültig: Es wird ein Dialogfenster mit den Zertifikatsinformationen angezeigt. Makros können nur dann aktiviert werden, wenn der Benutzer dem Autor und der Zertifizierungsstelle vertraut. Ein Netzwerkadministrator kann die Liste der vertrauenswürdigen Quellen sperren und damit verhindern, dass der Benutzer diese erweitert.
    - **Jeder Autor:** Signatur ist ungültig – möglicherweise aufgrund eines Virus. Der Benutzer wird vor einem möglichen Virus gewarnt. Makros sind automatisch deaktiviert.
    - **Jeder Autor:** Signaturprüfung ist nicht möglich, da der öffentliche Schlüssel fehlt oder ein inkompatibles Verschlüsselungsverfahren verwendet wurde. Der Benutzer wird gewarnt, dass eine Signaturprüfung nicht möglich ist. Makros sind automatisch deaktiviert.
    - **Jeder Autor:** Die Signatur wurde erstellt, nachdem das Zertifikat abgelaufen war oder zurückgezogen wurde. Der Benutzer wird gewarnt, dass die Signatur abgelaufen ist oder zurückgezogen wurde. Makros sind automatisch deaktiviert.
  - **Medium**
    - **Unsignierte Makros:** Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
    - **Signierte Makros:** Die Quelle und die Signatur des Makros legen fest, wie dieses gehandhabt wird.
    - **Vertrauenswürdige Quelle:** Signatur ist gültig: Makros sind automatisch aktiviert, und die Datei wird geöffnet.
    - **Unbekannter Autor:** Signatur ist gültig: Es wird ein Dialogfenster mit den Zertifikatsinformationen angezeigt. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren. Er kann dem Ersteller und der Zertifizierungsstelle vertrauen oder auch nicht.

        - **Jeder Autor:** Signatur ist ungültig – möglicherweise aufgrund eines Virus. Der Benutzer wird vor einem möglichen Virus gewarnt. Makros sind automatisch deaktiviert.
        - **Jeder Autor:** Signaturprüfung ist nicht möglich, da der öffentliche Schlüssel fehlt oder ein inkompatibles Verschlüsselungsverfahren verwendet wurde. Der Benutzer wird gewarnt, dass eine Signaturprüfung nicht möglich ist. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
        - **Jeder Autor:** Die Signatur wurde erstellt, nachdem das Zertifikat abgelaufen war oder zurückgezogen wurde. Der Benutzer wird gewarnt, dass die Signatur abgelaufen ist oder zurückgezogen wurde. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
    - **Low:** Alle Makros werden gleich behandelt – unabhängig von deren Quelle und Status. Es gibt keine Benachrichtigungen oder Signaturüberprüfungen. Makros werden automatisch aktiviert. Verwenden Sie die Einstellung nur, wenn Sie sicher sind, dass die Makros aller Dateien aus vertrauenswürdigen Quellen stammen.
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

In der Vergangenheit gab es viele Viren und Würmer, die als Makros in Office-Dokumenten entwickelt wurden. Ein Wurm ist ein Programm, das unabhängig arbeitet und sich über Netzwerkverbindungen von Computer zu Computer verbreitet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Medium**.

Mögliche Auswirkungen

Benutzern wird bei jedem Laden von unsignierten Makros oder bei signierten Makros, bei denen ein Problem mit dem Autor oder dem Zertifikat besteht, eine Fehlermeldung angezeigt. Makros mit ungültigen Signaturen werden deaktiviert.

Excel: Zugriff auf Visual Basic Project gestatten

Diese Einstellung legt fest, ob Excel Zugriff auf den VBA-Code von Dokumenten hat.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wie bei Makros auch, kann der VBA-Code Viren und Würmer enthalten.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

VBA-Code in Office-Dokumenten wird nicht ausgeführt.

Excel: Installierten Add-ins und Vorlagen vertrauen

Abhängig von den Makro-Sicherheitseinstellungen, wird ein Makro beim Öffnen deaktiviert, und Sie erhalten eine Mitteilung. Alle Makros, die mit Office XP installiert werden, sind von Microsoft signiert. Nachdem Sie für eins dieser Makros Microsoft zur Liste der vertrauenswürdigen Quellen hinzugefügt haben und die Einstellung **Excel: Installierten Add-ins und Vorlagen vertrauen** aktiviert haben, sollte bei deren Verwendung keine Benachrichtigung mehr auftreten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Sie haben die Möglichkeit, allen momentan installierten Add-Ins und Vorlagen zu vertrauen. Damit wird allen mit Microsoft Office installierten Dateien vertraut - unabhängig davon, ob diese signiert sind oder nicht. Es ist möglich, dass ein Angriff über einen Virus, ein Trojanisches Pferd oder anderen feindlichen Code eingebettet in ein Office-Dokument, stattfindet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Es gibt keinen direkten Weg, im Voraus eine Liste von vertrauenswürdigen Quellen zu laden. Sie müssen jedes Zertifikat erst auf einem Testcomputer akzeptieren. Dies kann viel Zeit in Anspruch nehmen.

Outlook: Makro Sicherheitsebene

E-Mails, die Sie auf Ihrem Computer erhalten, könnten Makros und Scripts mit Viren enthalten. Um Ihren Computer gegen solche Viren zu schützen, ist die Standard-Sicherheitseinstellung von Outlook **Hoch**.

Die möglichen Werte dieser Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
    - **Hoch:** Dies ist die Standardeinstellung. Sie können nur Makros ausführen, die signiert sind und aus einer vertrauenswürdigen Quelle stammen. Bevor Sie einer Quelle vertrauen, sollten Sie deren Arbeitsweise überprüfen, da Outlook Makros aus vertrauenswürdigen Quellen ohne jede Warnung ausführt.
    - **Mittel:** Bei einem Makro aus einer Quelle, die nicht in Ihrer Liste vertrauenswürdigen Quellen steht, zeigt Outlook eine Warnmeldung an. Sie können dies dann aktivieren oder deaktivieren.

    - **Gering:** Wählen Sie diese Einstellung nur, wenn Sie sicher sind, dass alle von Ihnen geöffneten Makros sicher sind. Sie stellt den Makroschutz von Outlook aus. Alle Makros werden ausgeführt.
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Outlook ist nicht in der Lage, Disketten, Festplatten oder Netzlaufwerke auf Makroviren zu prüfen. Wenn Sie eine solche Funktionalität benötigen, müssen Sie einen Virenscanner einsetzen.

Sicherheitslücken

In der Vergangenheit gab es viele Viren und Würmer, die als Makros in Office-Dokumenten entwickelt wurden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **High**.

Mögliche Auswirkungen

Nur signierte Makros aus vertrauenswürdigen Quellen werden ausgeführt.

PowerPoint: Makro Sicherheitsebene

Diese Einstellung legt den Virenschutz in PowerPoint fest.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
    - **Hoch**
        - **Unsignierte Makros**: Makros sind automatisch deaktiviert und die Datei wird geöffnet.
        - **Signierte Makros:** Die Quelle und die Signatur des Makros legen fest, wie dieses gehandhabt wird.
        - **Vertrauenswürdige Quelle:** Signatur ist gültig: Makros sind automatisch aktiviert und die Datei wird geöffnet.
        - **Unbekannter Autor:** Signatur ist gültig: Es wird ein Dialogfenster mit den Zertifikatsinformationen angezeigt. Makros können nur dann aktiviert werden, wenn der Benutzer dem Autor und der Zertifizierungsstelle vertraut. Ein Netzwerkadministrator kann die Liste der vertrauenswürdigen Quellen sperren, und damit verhindern, dass der Benutzer diese erweitert.
        - **Jeder Autor:** Signatur ist ungültig - möglicherweise aufgrund eines Virus. Der Benutzer wird vor einem möglichen Virus gewarnt. Makros sind automatisch deaktiviert.
        - **Jeder Autor:** Signaturenprüfung ist nicht möglich, da der öffentliche Schlüssel fehlt oder ein inkompatibles Verschlüsselungsverfahren verwendet wurde. Der Benutzer wird gewarnt, dass eine Signaturprüfung nicht möglich ist. Makros sind automatisch deaktiviert.
        - **Jeder Autor:** Die Signatur wurde erstellt, nachdem das Zertifikat abgelaufen war oder zurückgezogen wurde. Der Benutzer wird gewarnt, dass die Signatur abgelaufen ist oder zurückgezogen wurde. Makros sind automatisch deaktiviert.

- **Medium**
  - **Unsignierte Makros:** Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
  - **Signierte Makros:** Die Quelle und die Signatur des Makros legen fest, wie dieses gehandhabt wird.
  - **Vertrauenswürdige Quelle:** Signatur ist gültig: Makros sind automatisch aktiviert und die Datei wird geöffnet.
  - **Unbekannter Autor:** Signatur ist gültig: Es wird ein Dialogfenster mit den Zertifikatsinformationen angezeigt. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren. Er kann dem Ersteller und der Zertifizierungsstelle vertrauen oder auch nicht.
  - **Jeder Autor:** Signatur ist ungültig – möglicherweise aufgrund eines Virus. Der Benutzer wird vor einem möglichen Virus gewarnt. Makros sind automatisch deaktiviert.
  - **Jeder Autor:** Signaturenprüfung ist nicht möglich, da der öffentliche Schlüssel fehlt oder ein inkompatibles Verschlüsselungsverfahren verwendet wurde. Der Benutzer wird gewarnt, dass eine Signaturprüfung nicht möglich ist. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
  - **Jeder Autor:** Die Signatur wurde erstellt, nachdem das Zertifikat abgelaufen war oder zurückgezogen wurde. Der Benutzer wird gewarnt, dass die Signatur abgelaufen ist oder zurückgezogen wurde. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
- **Low:** Alle Makros werden gleich behandelt - unabhängig von deren Quelle und Status. Es gibt keine Benachrichtigungen oder Signaturüberprüfungen. Makros werden automatisch aktiviert. Verwenden Sie die Einstellung nur, wenn Sie sicher sind, dass die Makros aller Dateien aus vertrauenswürdigen Quellen stammen.

- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

In der Vergangenheit gab es viele Viren und Würmer, die als Makros in Office-Dokumenten entwickelt wurden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Medium**.

Mögliche Auswirkungen

Benutzern wird bei jedem Laden von unsignierten Makros oder bei signierten Makros, bei denen ein Problem mit dem Autor oder dem Zertifikat besteht, eine Fehlermeldung angezeigt. Makros mit ungültigen Signaturen werden deaktiviert.

PowerPoint: Zugriff auf Visual Basic Project gestatten

Diese Einstellung legt fest, ob PowerPoint Zugriff auf den VBA-Code von Dokumenten hat.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**

- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wie bei Makros auch, kann der VBA-Code Viren und Würmer enthalten.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

VBA-Code in Office-Dokumenten wird nicht ausgeführt.

PowerPoint: Allen installierten Add-ins und Vorlagen vertrauen

Abhängig von den Makro-Sicherheitseinstellungen wird ein Makro beim Öffnen deaktiviert, und Sie erhalten eine Mitteilung. Alle Makros, die mit Office XP installiert werden, sind von Microsoft signiert. Nachdem Sie für eins dieser Makros Microsoft zur Liste der vertrauenswürdigen Quellen hinzugefügt haben und die Einstellung **PowerPoint: Allen installierten Add-ins und Vorlagen vertrauen** aktiviert haben, sollte bei deren Verwendung keine Benachrichtigung mehr auftreten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Sie haben die Möglichkeit, allen momentan installierten Add-Ins und Vorlagen zu vertrauen. Damit wird allen mit Microsoft Office installierten Dateien vertraut. Ob diese signiert sind oder nicht. Es ist möglich, dass ein Angriff über einen Virus, ein Trojanisches Pferd oder anderen feindlichen Code eingebettet in ein Office-Dokument, stattfindet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Es gibt keinen direkten Weg, im vorab eine Liste von vertrauenswürdigen Quellen zu laden. Sie müssen jedes Zertifikat erst auf einem Testcomputer akzeptieren. Dies kann viel Zeit in Anspruch nehmen.

Unsichere ActiveX-Initialisierung

Über diese Einstellung können Sie festlegen, wie ActiveX-Steuerelemente in Office XP Anwendungen aktiviert werden. ActiveX-Steuerelemente stellen über Office XP und den Internet Explorer

umfangreiche Funktionalität zu Verfügung. Da sie aber ausführbare Codestücke sind, könnte ein böswilliger Entwickler ActiveX-Steuerelemente erstellen, die unerwünschte Aktionen durchführen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Initialize using control defaults** (Initialisierung mit den Standardeinstellung des Steuerelements)
  - **Ask user: persisted data or control defaults** (Benutzerdefiniert: Schreibgeschützte Daten oder Standardeinstellungen des Steuerelements)
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Um gegen schädliche Steuerelemente geschützt zu sein, kann Office XP so konfiguriert werden, dass Endbenutzer nur digital signierte Steuerelemente ausführen können.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** und **Initialize using control defaults.**

Mögliche Auswirkungen

Da die Einstellung bewirkt, dass die durch ein Steuerelement gespeicherten Daten bei jedem Start des Steuerelements verworfen werden, kann Sie zu Problemen beim Anzeigen von Dokumenten führen.

Word: Makro-Sicherheitsebene

Diese Einstellung legt den Virenschutz in Word fest.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Hoch**
    - **Unsignierte Makros**: Makros sind automatisch deaktiviert und die Datei wird geöffnet.
    - **Signierte Makros:** Die Quelle und die Signatur des Makros legen fest, wie dieses gehandhabt wird.
    - **Vertrauenswürdige Quelle:** Signatur ist gültig: Makros sind automatisch aktiviert, und die Datei wird geöffnet.
    - **Unbekannter Autor:** Signatur ist gültig: Es wird ein Dialogfenster mit den Zertifikatsinformationen angezeigt. Makros können nur dann aktiviert werden, wenn der Benutzer dem Autor und der Zertifizierungsstelle vertraut. Ein Netzwerkadministrator kann die Liste der vertrauenswürdigen Quellen sperren und damit verhindern, dass der Benutzer diese erweitert.
    - **Jeder Autor:** Signatur ist ungültig – möglicherweise aufgrund eines Virus. Der Benutzer wird vor einem möglichen Virus gewarnt. Makros sind automatisch deaktiviert.
    - **Jeder Autor:** Signaturprüfung ist nicht möglich, da der öffentliche Schlüssel fehlt oder ein inkompatibles Verschlüsselungsverfahren verwendet wurde. Der Benutzer wird gewarnt, dass eine Signaturprüfung nicht möglich ist. Makros sind automatisch deaktiviert.

        - **Jeder Autor:** Die Signatur wurde erstellt, nachdem das Zertifikat abgelaufen war oder zurückgezogen wurde. Der Benutzer wird gewarnt, dass die Signatur abgelaufen ist oder zurückgezogen wurde. Makros sind automatisch deaktiviert.
    - **Medium**
        - **Unsignierte Makros:** Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
        - **Signierte Makros:** Die Quelle und die Signatur des Makros legen fest, wie dieses gehandhabt wird.
        - **Vertrauenswürdige Quelle:** Signatur ist gültig: Makros sind automatisch aktiviert, und die Datei wird geöffnet.
        - **Unbekannter Autor:** Signatur ist gültig: Es wird ein Dialogfenster mit den Zertifikatsinformationen angezeigt. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren. Er kann dem Ersteller und der Zertifizierungsstelle vertrauen oder auch nicht.
        - **Jeder Autor:** Signatur ist ungültig – möglicherweise aufgrund eines Virus. Der Benutzer wird vor einem möglichen Virus gewarnt. Makros sind automatisch deaktiviert.
        - **Jeder Autor:** Signaturprüfung ist nicht möglich, da der öffentliche Schlüssel fehlt oder ein inkompatibles Verschlüsselungsverfahren verwendet wurde. Der Benutzer wird gewarnt, dass eine Signaturprüfung nicht möglich ist. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
        - **Jeder Autor:** Die Signatur wurde erstellt, nachdem das Zertifikat abgelaufen war oder zurückgezogen wurde. Der Benutzer wird gewarnt, dass die Signatur abgelaufen ist oder zurückgezogen wurde. Der Benutzer wird aufgefordert Makros zu aktivieren oder zu deaktivieren.
    - **Low:** Alle Makros werden gleich behandelt - unabhängig von deren Quelle und Status. Es gibt keine Benachrichtigungen oder Signaturüberprüfungen. Makros werden automatisch aktiviert. Verwenden Sie die Einstellung nur wenn Sie sicher sind, dass die Makros aller Dateien aus vertrauenswürdigen Quellen stammen.
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

In der Vergangenheit gab es viele Viren und Würmer, die als Makros in Office-Dokumenten entwickelt wurden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Medium**.

Mögliche Auswirkungen

Benutzern wird bei jedem Laden von unsignierten Makros oder bei signierten Makros, bei denen ein Problem mit dem Autor oder dem Zertifikat besteht, eine Fehlermeldung angezeigt. Makros mit ungültigen Signaturen werden deaktiviert.

Word: Allen installierten Add-ins und Vorlagen vertrauen

Abhängig von den Makro-Sicherheitseinstellungen wird ein Makro beim Öffnen deaktiviert und Sie

erhalten eine Mitteilung. Alle Makros, die mit Office XP installiert werden, sind von Microsoft signiert. Nachdem Sie für eins dieser Makros Microsoft zur Liste der vertrauenswürdigen Quellen hinzugefügt haben und die Einstellung **Word: Allen installierten Add-ins und Vorlagen vertrauen** aktiviert haben, sollte bei deren Verwendung keine Benachrichtigung mehr auftreten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Sie haben die Möglichkeit, allen momentan installierten Add-Ins und Vorlagen zu vertrauen. Damit wird allen mit Microsoft Office installierten Dateien vertraut – unabhängig davon, ob diese signiert sind oder nicht. Es ist möglich, dass ein Angriff über einen Virus, ein Trojanisches Pferd oder anderen feindlichen Code eingebettet in ein Office-Dokument, stattfindet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Es gibt keinen direkten Weg, im vorab eine Liste von vertrauenswürdigen Quellen zu laden. Sie müssen jedes Zertifikat erst auf einem Testcomputer akzeptieren. Dies kann viel Zeit in Anspruch nehmen.

Word: Allen installierten Add-ins und Vorlagen vertrauen

Abhängig von den Makro-Sicherheitseinstellungen wird ein Makro beim Öffnen deaktiviert, und Sie erhalten eine Mitteilung. Alle Makros, die mit Office XP installiert werden, sind von Microsoft signiert. Nachdem Sie für eins dieser Makros Microsoft zur Liste der vertrauenswürdigen Quellen hinzugefügt haben und die Einstellung **Word: Allen installierten Add-ins und Vorlagen vertrauen** aktiviert haben, sollte bei deren Verwendung keine Benachrichtigung mehr auftreten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Sie haben die Möglichkeit, allen momentan installierten Add-Ins und Vorlagen zu vertrauen. Damit wird allen mit Microsoft Office installierten Dateien vertraut – unabhängig davon, ob diese signiert sind oder nicht. Es ist möglich, dass ein Angriff über einen Virus, ein Trojanisches Pferd oder anderen feindlichen Code eingebettet in ein Office-Dokument, stattfindet.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **deaktiviert**.

Mögliche Auswirkungen

Es gibt keinen direkten Weg, im vorab eine Liste von vertrauenswürdigen Quellen zu laden. Sie müssen jedes Zertifikat erst auf einem Testcomputer akzeptieren. Dies kann viel Zeit in Anspruch nehmen.

Verarbeitung von Gruppenrichtlinien

Sie können die Verarbeitungsreihenfolge von Gruppenrichtlinien über die Einstellungen im folgenden Pfad anpassen:
Computerkonfiguration\Administrative Vorlagen\System\Gruppenrichtlinien

Verarbeitung von Registrierungsrichtlinien

Diese Einstellung legt fest, wann die Registrierungsrichtlinien aktualisiert werden. Sie betrifft alle Richtlinien im Ordner **administrative Vorlagen** und alle anderen Richtlinien, die Werte der Registrierung ändern. Die Einstellung **Nicht bei der Hintergrundaktualisierung anwenden** verhindert die Hintergrundaktualisierung der Richtlinien. Diese könnte die Arbeit des Benutzers unterbrechen und - in seltenen Fällen - Daten beschädigen. Wenn die Einstellung auf den Wert **Anwenden, auch wenn die Gruppenrichtlinienobjekte nicht geändert wurden** gesetzt ist, werden auch die nicht geänderten Richtlinien neu angewandt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Nicht bei der Hintergrundaktualisierung anwenden**
  - **Anwenden, auch wenn die Gruppenrichtlinienobjekte nicht geändert wurden**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn diese Einstellung auf **Anwenden, auch wenn die Gruppenrichtlinienobjekte nicht geändert wurden** konfiguriert ist, ist sichergestellt, dass die Richtlinien auch dann aktualisiert werden, wenn keine Änderungen vorhanden sind. Auf diese Weise werden alle lokalen Änderungen regelmäßig von den domänenbasierten Gruppernrichtlinien-Einstellungen überschrieben.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** und **Anwenden, auch wenn die Gruppenrichtlinienobjekte nicht geändert wurden**.

Mögliche Auswirkungen

Gruppenrichtlinien werden bei jeder Aktualisierung neu angewandt. Dies könnte geringe Auswirkungen auf die Leistung haben.

Verarbeitung der Richtlinien für die Internet Explorer-Wartung

Diese Einstellung legt fest, wann die Richtlinien für die Internet Explorer-Wartung aktualisiert werden. Sie betrifft alle Richtlinien im Ordner Internet Explorer Maintenance.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
    - **Verarbeitung bei langsamen Netzwerkverbindungen gestatten:** Diese Option aktualisiert die Richtlinien auch dann, wenn diese über eine langsame Netzwerkverbindung übertragen werden. Dies kann zu deutlichen Verzögerungen führen.
    - **Nicht bei der Hintergrundaktualisierung anwenden:** Diese Option verhindert, dass die betroffenen Richtlinien während der Verwendung des Computers aktualisiert werden. Eine Hintergrundaktualisierung könnte zur Unterbrechung der Arbeit des Benutzers führen und - in seltenen Fällen - zu einem Datenverlust.
    - **Anwenden, auch wenn die Gruppenrichtlinienobjekte nicht geändert wurden:** Die Option aktualisiert die Richtlinien und wendet diese neu an. Dies passiert auch dann, wenn sich die Richtlinien nicht geändert haben.
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Indem Sie die Einstellung mit der Option **Process even if the Group Policy objects have not changed** verwenden, stellen Sie sicher, dass die Richtlinien auch dann neu angewandt werden, wenn sich diese nicht verändert haben. So stellen Sie sicher, dass alle lokalen Änderungen von den Gruppenrichtlinien der Domäne überschrieben werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** mit der Option **Process even if the Group Policy objects have not changed**. **Mögliche Auswirkungen**.

Fehlerberichterstattung

Die Fehlerberichterstattung ermöglicht es Administratoren die Cabinet-Dateien, die durch DW.exe erstellt werden zu verwalten und Stop-Fehlermeldung auf einen lokalen Dateiserver umzuleiten. Sie können die Einstellungen der Fehlerberichterstattung über den folgenden Pfad konfigurieren: *Computerkonfiguration\Administrative Vorlagen\System\Fehlerberichterstattung*

Fehlerbenachrichtung anzeigen

Über diese Einstellung können Sie bestimmen, ob dem Benutzer Fehlermeldungen angezeigt werden. Wenn sie aktiviert ist, wird der Benutzer bei Fehlern benachrichtigt und kann selbst auswählen, ob der Fehler weitergeleitet werden soll oder nicht. Ist die Einstellung deaktiviert, kann der Benutzer nicht selbst entscheiden. Die Fehlerberichte werden automatisch weitergeleitet. Wird die Einstellung nicht konfiguriert, kann das Verhalten weiterhin lokal über die Systemsteuerung konfiguriert werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Wenn die Benutzer selbst entscheiden dürfen, ob Fehler weitergeleitet werden, könnten diese Entscheidungen treffen, die nicht mit den Unternehmensrichtlinien übereinstimmen.

Gegenmaßnahmen

Setzen Sie die Einstellungen auf **Deaktiviert**.

Mögliche Auswirkungen

Benutzer werden keine Fehlermeldungen mehr angezeigt.

Fehler melden

Diese Einstellung legt fest, ob Fehler weitergeleitet werden. Wenn sie aktiviert ist, kann der Benutzer entscheiden, ob ein Fehler weitergeleitet wird.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit den folgenden Optionen:**
  - **Keine von Microsoft angebotenen Websites bezüglich „weiterer Informationen“ anzeigen.**
  - **Keine zusätzlichen Dateien sammeln.**
  - **Keine zusätzlichen Computerdaten sammeln.**
  - **Warteschlangenmodus für Anwendungsfehler erzwingen:** Mit dieser Option kann der Benutzer nicht mehr wählen, ob er einen Fehlerbericht senden möchte. Stattdessen wird der Fehler an eine Warteschlange gesendet. Der nächste Administrator, der sich anmeldet, muss entscheiden, ob der Fehler gesendet wird.
  - **Dateiuploadpfad für zentrale Fehlerberichte:** Bei dieser Option können Sie einen UNC-Pfad angeben, in den die Fehlerberichte hochgeladen werden.
  - **Instanzen des Worts "Microsoft" ersetzen durch.**
- **Deaktiviert**
- **Nicht konfiguriert**

Wenn diese Einstellung nicht konfiguriert wird, kann der Benutzer sie selbst über die Systemsteuerung konfigurieren.

Sicherheitslücken

Das Fehlerberichterstattungs-Feature von Windows XP, Windows Server 2003 und Office XP sendet normalerweise Daten an Microsoft, die einige Unternehmen lieber vertraulich behandeln möchten. Die Datenschutzvereinbarung von Microsoft stellt sicher, dass Microsoft diese gesammelten Daten nicht missbraucht. Trotzdem mag es sein, das einige Organisationen keine Daten ohne eine vorherige Prüfung durch Mitglieder des IT-Teams senden möchten, andererseits jedoch die Fehlerberichterstattung nicht komplett deaktivierten möchten, da Microsoft die Informationen zur Erkennung und zur Diagnose von Fehlern verwendet. Ein Verfahren, um beides sicherzustellen ist das Einrichten eines internen Fehlerberichterstattungs-Servers (Corporate Error Reporting - CER). Sie können die Clientcomputer dann so konfigurieren, dass diese die Fehlerberichte an den Server senden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert,** und Tragen unter **Dateiuploadpfad für zentrale Fehlerberichte** den UNC-Pfad des CER-Servers ein.

> **Anmerkung:** Weitere Informationen zur Einrichtung von CER-Servern finden Sie auf der Office Resource Kit Webseite unter http://www.microsoft.com/office/ork/xp/appndx/appa19.htm (englischsprachig).

Mögliche Auswirkungen

Die Fehlerberichterstattung ist aktiviert. Die Fehlerberichte werden an den CER-Server gesendet.

Internet Explorer Benutzereinstellungen

Viele der Einstellungen des Internet Explorers können Sie über den folgenden Pfad einer Gruppenrichtlinie konfigurieren:
Benutzerkonfiguration\Administrative Vorlagen\Windows Komponenten\Internet Explorer

Menü "Datei": Menüoption "Speichern unter..." deaktivieren

Die Aktivierung dieser Einstellung verhindert, dass Benutzer Dateien beim Herunterladen speichern können. Die Datei wird nicht heruntergeladen und der Benutzer wird darüber informiert.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten Dateien herunterladen und ausführen, die bösartigen Programmcode enthalten.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht in der Lage Dateien herunterzuladen.

Outlook Express konfigurieren

Diese Einstellung ermöglicht es Administratoren den Benutzern die Möglichkeit zu nehmen, Dateianhänge in Microsoft Outlook® Express zu speichern. Diese könnten zum Beispiel Viren enthalten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert – mit der folgenden Option:**
  - **Anhänge die Viren enthalten können blockieren**

- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer, die E-Mail öffnen, könnten unbeabsichtigt bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert** und **Anhänge die Viren enthalten können blockieren**.

Mögliche Auswirkungen

Benutzer sind nicht in der Lage, in Outlook Express Anhänge auszuführen oder zu speichern.

Einstellungen für die Seite "Erweitert" deaktivieren

Diese Einstellung verhindert, dass Benutzer die Einstellungen auf der Seite „Erweitert“ im Dialogfenster „Internetoptionen“ ändern.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Die Benutzer sind nicht in der Lage, die Einstellungen auf der Registerkarte „Erweitert“ im Dialogfenster „Internetoptionen“ zu verändern.

Änderung der Einstellungen für automatische Konfiguration deaktivieren

Diese Einstellung verhindert, dass Benutzer die automatischen Konfigurationseinstellungen verändern. Die automatische Konfiguration ist ein Verfahren, über das Administratoren die Browsereinstellungen regelmäßig aktualisieren können. Sie finden diese im Bereich *Automatische Konfiguration* des Dialogfensters **Local Area Network (LAN) Einstellungen**.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**

- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Die Benutzer sind nicht in der Lage, die Einstellungen für die automatische Konfiguration zu verändern.

Änderung der Zertifikateinstellungen deaktivieren

Diese Einstellung verhindert, dass Benutzer die Zertifikatseinstellung des Internet Explorers ändern. Zertifikate werden verwendet, um die Identität von Softwareanbietern zu prüfen. Wenn die Einstellung aktiviert ist, kann der Benutzer auf die Registerkarte *Inhalte* des Dialogfensters *Internetoptionen* auf den Bereich *Zertifikate* nicht mehr zugreifen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Achtung: Die Aktivierung dieser Richtlinie verhindert nicht, das Benutzer den Zertifikatsverwaltungsassistenten ausführen, indem sie doppelt auf eine Zertifikatskonfigurationsdateien (.spc) klicken. Dieser Assistent ermöglicht es Benutzern, die Einstellungen für neue Zertifikate zu konfigurieren.

Sicherheitslücken

Benutzer könnten neue Zertifikate importieren, bestätigte Zertifikate entfernen, oder deren Einstellungen verändern. Dies könnte zum Fehlschlag von bestätigten Anwendungen oder der Ausführung von nicht bestätigten Anwendungen führen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die Zertifikatseinstellungen zu verändern.

Änderung der Verbindungseinstellungen deaktivieren

Diese Einstellung verhindert, dass Benutzer die Einstellungen der Einwählverbindungen ändern. Wenn die Einstellung aktiviert ist, kann der Benutzer auf die Registerkarte *Verbindungen* des Dialogfensters *Internetoptionen* nicht mehr zugreifen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer können bestehende Verbindungen verändern und so den Zugriff auf Webseiten verhindern.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die Verbindungseinstellungen zu verändern.

Änderung der Proxy-Einstellungen deaktivieren

Diese Einstellung verhindert, dass Benutzer die Proxy-Einstellungen ändern.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer können bestehende Proxy-Einstellungen verändern und so den Zugriff auf Webseiten verhindern.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die Proxy-Einstellungen zu verändern.

Assistenten für Internetzugang deaktivieren

Diese Einstellung verhindert, dass Benutzer den Internetverbindungsassistenten ausführen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer können über den Internetverbindungsassistenten neue Internetverbindungen erstellen. So könnte das Unternehmensnetzwerk angreifbar werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer können den Internetverbindungsassistenten nicht verwenden.

Kennwörter in AutoVervollständigen können nicht gespeichert werden

Diese Einstellung deaktiviert die automatische Vervollständigung von Benutzernamen und Passwörtern in Formularen auf Webseiten. Außerdem werden die Benutzer nicht mehr gefragt, ob sie Passwörter speichern möchten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Das AutoVervollständigen Feature ist sehr nützlich. Es speichert Passwörter in geschütztem Speicher. Hierbei handelt es sich zwar um einen sehr sicheren Schutz, per Definition muss die gespeicherte Information jedoch mindestens für denjenigen abrufbar sein, der sie gespeichert hat. Es gibt inzwischen Tools im Internet, die den Inhalt des geschützten Speichers des Benutzers anzeigen. Sie können zwar nicht verwendet werden, um den Inhalt des geschützten Speichers eines anderen Benutzers anzuzeigen, ein Benutzer, der eins dieser Tools versehendlich ausführt, könnte jedoch sein Passwort ungewollt einem Angreifer anzeigen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, Passwörter über die AutoVervollständigen-Funktion zu speichern.

Internetsystemsteuerung: Seite "Erweitert" deaktivieren

Wenn Sie diese Einstellung aktivieren, kann der Benutzer auf die Registerkarte *Erweitert* des Dialogfensters *Internetoptionen* nicht mehr zugreifen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die erweiterten Einstellungen zu verändern.

Internetsystemsteuerung: Seite "Sicherheit" deaktivieren

Diese Einstellung entfernt die Registerkarte *Sicherheit* aus dem Dialogfenster *Internetoptionen.*

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die Sicherheitseinstellungen zu verändern.

Offlineseiten: Entfernen von Channels deaktivieren

Diese Einstellung verhindert, dass Benutzer Channels entfernen. Channels sind Webseiten, die auf dem Computer nach einem Zeitplan automatisch von Channelprovider aktualisiert werden.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Es könnten ohne direkte Interaktion des Benutzers Daten an dessen Browser gesendet werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer können keine Channels entfernen.

Offlineseiten: Hinzufügen von Zeitplänen für Offlineseiten deaktivieren

Diese Einstellung verhindert, dass Benutzer Webseiten für eine Offlineanzeige definieren. Sie erzeugt durch das Herunterladen der Offlineinhalte Serverlast.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die Zeitpläne für Offlineseiten zu erstellen.

Offlineseiten: Alle geplanten Offlineseiten deaktivieren

Diese Einstellung deaktiviert bestehende Zeitpläne für Offlineseiten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**

- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die Zeitpläne für Offlineseiten anzuzeigen.

Offlineseiten: Channel-Benutzeroberfläche vollständig deaktivieren

Diese Einstellung verhindert, dass die Benutzer auf die Channeleinstellungen zugreifen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, auf die Channel-Benutzerschnittstelle zuzugreifen.

Offlineseiten: Download von abonnierten Siteinhalten deaktivieren

Diese Einstellung verhindert, dass Benutzer Inhalte von Webseiten herunterladen, die sie abonniert haben. Die Synchronisation mit diesen Webseiten findet jedoch trotzdem statt.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**

- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, über Seitenabonnements Inhalte herunterzuladen.

Offlineseiten: Das Bearbeiten und Erstellen von geplanten Gruppen deaktivieren

Diese Einstellung verhindert, dass Benutzer Zeitpläne für die Offlinenutzung von Webseiten erstellen, ändern oder löschen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, Zeitpläne zu erstellen, zu ändern oder zu entfernen.

Offlineseiten: Bearbeiten von Zeitplänen für Offlineseiten deaktivieren

Diese Einstellung verhindert, dass Benutzer die bestehenden Zeitpläne verändern.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, Zeitpläne zu bearbeiten.

Offlineseiten: Trefferprotokollierung für Offlineseiten deaktivieren

Diese Einstellung verhindert, dass Channelprovider Informationen darüber erlangen, wann die Channelseiten von den Offlinebenutzern angezeigt wurden. Wenn die Einstellung aktiviert ist, deaktiviert sie alle Channel-Protokolleinstellungen die von Channelprovidern über das Channel Definition Format (.cdf) konfiguriert wurden. Die .cdf-Dateien legen den Zeitplan und andere Einstellungen für das Herunterladen von Webinhalten fest.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Die Trefferprotokolle werden für Benutzer, die ohne Verbindung auf Seiten zugreifen, nicht mehr an die entsprechenden Webseiten weitergeleitet.

Offlineseiten: Entfernen von Channels deaktivieren

Diese Einstellung verhindert, dass Benutzer die Channelsynchronisierung im Internet Explorer deaktivieren.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**

- **Nicht konfiguriert**

Anmerkung: Diese Richtlinie verhindert nicht, dass Benutzer aktive Inhalte vom Desktop entfernen.

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, Channels zu entfernen oder die Channelsynchronisation zu verhindern

Offlineseiten: Entfernen von Zeitplänen für Offlineseiten deaktivieren

Diese Einstellung verhindert, dass Benutzer die vorgegebenen Zeitpläne für die Offlineanzeige von Webseiten verändern oder löschen.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Benutzer könnten die Sicherheitseinstellungen des Internet Explorers ändern. Dies könnte dazu führen, dass die Benutzer schädliche Webseiten aufrufen oder bösartigen Programmcode ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer sind nicht mehr in der Lage, die Zeitpläne für Offlineseiten zu entfernen.

Bildschirmschoner-Einstellungen

Bildschirmschoner wurden ursprünglich zum Schutz der Kathodenstrahlröhren von Monitoren entwickelt. Sie haben sich im Lauf der Zeit zu einem Sicherheitswerkzeug weiterentwickelt, indem sie den Bildschirm automatisch sperren, wenn der Benutzer seinen Arbeitsplatz verlässt und vergisst diesen zu sperren. Die Einstellungen für Bildschirmschoner können über den folgenden Pfad konfiguriert werden:

Benutzerkonfiguration\Administrative Vorlagen\Systemsteuerung\Anzeige

Kennwortschutz für den Bildschirmschoner verwenden

Diese Einstellung legt fest, ob der Bildschirmschoner durch ein Passwort geschützt ist. Ist sie aktiviert, dann ist das Kontrollkästchen **Passwortschutz** auf der Registerkarte *Bildschirmschoner* des Dialogfensters *Anzeigeeigenschaften* gesperrt. Der Passwortschutz ist dann aktiviert. Sie sollten zusätzlich die Einstellung **Bildschirmschoner Zeitlimit** konfigurieren.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Um die Registerkarte **Bildschirmschoner** vollständig zu entfernen, verwenden Sie die Einstellung **Registerkarte Bildschirmschoner entfernen**.

Sicherheitslücken

Wenn kein Passwortschutz für den Bildschirmschoner verwendet wird, und der Benutzer seinen Desktop nicht beim Verlassen des Arbeitsplatzes sperrt, dann ist die Arbeitsstation ungeschützt.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Benutzer müssen ihre Computer nach einem Start des Bildschirmschoners entsperren.

Bildschirmschoner

Diese Einstellung aktiviert den Bildschirmschoner. Wenn sie deaktiviert ist, wird kein Bildschirmschoner gestartet. Wenn die Einstellung aktiviert ist und die folgenden zwei Bedingungen zutreffen, dann wird der Bildschirmschoner verwendet: Im Feld **Bildschirmschoner** ist ein gültiger Bildschirmschoner angegeben, und im Feld **Wartezeit** ist ein Wert größer 0 angegeben.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Damit die oben beschriebenen Einstellungen verwendet werden können, muss diese Einstellung aktiviert sein.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Mögliche Auswirkungen

Diese Einstellung aktiviert die Bildschirmschoner auf den Computern der Umgebung.

Programmname des Bildschirmschoners

Diese Einstellung definiert den Bildschirmschoner, der ausgeführt wird. Wenn die Einstellung aktiviert ist, kann der Benutzer auf die Auswahlliste im Feld **Bildschirmschoner** nicht mehr zugreifen. Geben Sie den vollständigen Dateinamen des Bildschirmschoners an, inklusive der Dateiendung .scr. Wenn er sich nicht im Ordner *%Systemroot%\System32* befindet, müssen Sie außerdem den vollqualifizierten Pfad der Datei angeben.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert** – mit dem Namen der Datei des Bildschirmschoners.
- **Deaktiviert**
- **Nicht konfiguriert**

Anmerkung: Diese Einstellung kann durch die Einstellung **Bildschirmschoner** überschrieben werden. Wenn diese deaktiviert ist, wird kein Bildschirmschoner gestartet - unabhängig davon, ob hier eine Datei definiert ist.

Sicherheitslücken

Es muss ein gültiger Dateiname für einen Bildschirmschoner angegeben werden.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **scrnsave.scr** - dies ist der „Leerer Bildschirm“ Bildschirmschoner - oder einen Bildschirmschoner Ihrer Wahl.

Mögliche Auswirkungen

Der definierte Bildschirmschoner wird nach der konfigurierten Wartezeit ausgeführt.

Bildschirmschoner Zeitlimit

Diese Einstellung definiert, wie lange der Benutzer inaktiv sein muss, bevor der Bildschirmschoner gestartet wird. Der Wert kann zwischen 1 Sekunde und 86.000 Sekunden (24 Stunden) liegen. Die Einstellung hat unter den folgenden Bedingungen keine Auswirkungen:

- Sie ist deaktiviert oder nicht konfiguriert.
- Die Wartezeit ist auf 0 gesetzt.
- Die Einstellung **Kein Bildschirmschoner** ist Aktiviert.
- Es ist weder unter der Einstellung **Programmname des Bildschirmschoners**, noch im Feld **Bildschirmschoner** unter der Registerkarte **Bildschirmschoner** des Dialogfensters **Anzeigeeigenschaften** ein gültiger Bildschirmschoner angegeben.

Wenn die Einstellung nicht konfiguriert ist, wird die Wartezeit verwendet, die auf dem Client konfiguriert ist. Die Standardeinstellung ist hier 15 Minuten.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert** – mit einem benutzerdefinierten Wert zwischen 0 und 86.000 Sekunden.
- **Deaktiviert**
- **Nicht konfiguriert**

Sicherheitslücken

Damit der Bildschirmschoner aktiv wird, muss eine gültige Wartezeit konfiguriert sein.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **600 Sekunden**.

Mögliche Auswirkungen

Nach fünf Minuten Inaktivität des Benutzers wird der Bildschirmschoner gestartet.

10

Zusätzliche Registrierungseinträge

Dieses Kapitel beschreibt zusätzliche Registrierungseinträge. Hierbei handelt es sich um Einträge, die nicht in den administrativen Vorlagen (.adm Dateien) enthalten sind. Die .adm-Dateien definieren Systemrichtlinien und Einschränkungen bezüglich des Desktops, der Shell und der Sicherheit von Microsoft Windows Server 2003.

Das bedeutet, dass die nachfolgenden Registrierungsschlüssel und Werte im Snap-In *Sicherheitsvorlagen* der Microsoft Management Konsolen (MMC) nicht vorhanden sind. Stattdessen sind die Registrierungseinträge in eine .inf-Datei aufgenommen worden. Die Einträge können außerdem mit Hilfe eines Texteditors, wie zum Beispiel Notepad angezeigt und verändert werden.

Die Einstellungen sind in die Sicherheitsvorlagen eingebettet, damit eine automatische Änderung stattfindet. Sollte die Richtlinie entfernt werden, bleiben die Einstellungen allerdings bestehen. Sie müssen von Hand entfernt werden. Eine Möglichkeit hierzu bietet der Registrierungseditor Regedt32.exe. Die Excel-Datei *Windows Standardeinstellungen für Sicherheit und Dienste.xls* enthält die Standardwerte.

Wie Sie Veränderungen an der Benutzeroberfläche des Sicherheitskonfigurationseditors durchführen können

Der SCE definiert Sicherheitseinstellungen, die auf einzelne Computer oder mittels Gruppenrichtlinien auf mehrere Computer angewendet werden können. Diese Sicherheitsvorlagen können Einstellungen bezüglich der Kennwörter, Anmeldungen, Kerberoseinstellungen, Überwachungsrichtlinien, Ereignisprotokolleinstellungen, Registrierungseinträge, Startparameter verschiedener Systemdienste sowie Benutzerrechte, Gruppenmitgliedschaften, Zugriff auf die Registrierung und Dateiberechtigungen definieren. Folgende Verwaltungskonsolen nutzen die Informationen und erlauben eine Veränderung der Werte:

- Sicherheitskonfiguration und –analyse
- Gruppenrichtlinien
- Lokale Sicherheitsrichtlinie
- Sicherheitsrichtlinie für Domänen
- Sicherheitsrichtlinie für Domänenkontroller

Ferner können Sie sich die verschiedenen Vorlagen und deren Einstellungen, die von Microsoft entweder gleich mitinstalliert werden oder aber zum Herunterladen zur Verfügung stehen, mit dem Snap-In Sicherheitsvorlagen anzeigen lassen.

Dieses Handbuch stellt Ihnen zusätzliche Einträge zur Änderung der Sicherheitskonfiguration des Computers zur Verfügung. Dabei werden Einträge in der Datei *sceregvl.inf* verändert bzw. hinzugefügt. Die Datei finden Sie im *%systemroot%\inf* Ordner ihres Systems. Nach einer Veränderung der Werte muss die *scecli.dll* nochmals registriert werden. Alle Einstellungen können in der Managementkonsole *Lokale Sicherheitsrichtlinie* angezeigt und modifiziert werden. Auch alle weiter oben in diesem Kapitel erwähnten Snap-Ins ermöglichen einen Zugriff auf die eingestellten Sicherheitsparameter. Um alle Computer entweder separat oder über Gruppenrichtlinien zu aktualisieren, müssen Sie die Datei *sceregvl.inf* aktualisieren und anschließend die *scecli.dll* nochmals registrieren. Eine detaillierte Anweisung der Einzelschritte finden Sie weiter unten in diesem Abschnitt. Beachten Sie bitte, dass die hier beschriebenen Veränderungsmöglichkeiten nur für Windows® XP

Professional mit Service Pack 1 und Windows® Server 2003 unterstützt werden. Versuchen Sie nicht, diese Einstellungen für ältere Windows-Versionen zu konfigurieren.

Wenn die Datei *sceregvl.inf* verändert und registriert ist, können die veränderten Registrierungseinträge in der Benutzeroberfläche des SCE eines Computers angezeigt werden. Die Namen der Einträge fangen immer mit der Bezeichnung „MSS“ an. MSS steht für Microsoft Lösungen (Solutions) für Sicherheit (Security) und bezeichnet den Namen der Arbeitsgruppe, die dieses Handbuch herausgegeben hat. Mit Hilfe dieser Vorlagen können Sie neue Vorlagen und Richtlinien erstellen, die dann auf eine Vielzahl von Computern angewendet werden können. Dabei spielt es keine Rolle, ob auf dem Zielcomputer die Datei *sceregvl.inf* verändert wurde oder nicht.

Aktualisieren der Datei sceregvl.inf

7. Öffnen Sie die Datei *%systemroot%\inf\sceregvl.inf* mit einem Texteditor, zum Beispiel Notepad.
8. Blättern Sie zum Ende des Bereichs **[Register Registry Values]** und kopieren Sie den folgenden Text in die Datei:

```
;================================ MSS Values ================================
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect,4,%Enabl
eICMPRedirect%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect,4,%SynAtta
ckProtect%,3,0|%SynAttackProtect0%,1|%SynAttackProtect1%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect,4,%Enabl
eDeadGWDetect%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery,4,%Enab
lePMTUDiscovery%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime,4,%KeepAliveT
ime%,3,150000|%KeepAliveTime0%,300000|%KeepAliveTime1%,600000|%KeepAliveTime2%,1200000
|%KeepAliveTime3%,2400000|%KeepAliveTime4%,3600000|%KeepAliveTime5%,7200000|%KeepAlive
Time6%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting,4,%D
isableIPSourceRouting%,3,0|%DisableIPSourceRouting0%,1|%DisableIPSourceRouting1%,2|%Di
sableIPSourceRouting2%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetran
smissions,4,%TcpMaxConnectResponseRetransmissions%,3,0|%TcpMaxConnectResponseRetransmi
ssions0%,1|%TcpMaxConnectResponseRetransmissions1%,2|%TcpMaxConnectResponseRetransmiss
ions2%,3|%TcpMaxConnectResponseRetransmissions3%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions,4
,%TcpMaxDataRetransmissions%,1
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery,4,%P
erformRouterDiscovery%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TCPMaxPortsExhausted,4,%TCP
MaxPortsExhausted%,1
MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand,4,%No
NameReleaseOnDemand%,0
MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation,4,%Nt
fsDisable8dot3NameCreation%,0
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun
,4,%NoDriveTypeAutoRun%,3,0|%NoDriveTypeAutoRun0%,255|%NoDriveTypeAutoRun1%
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel,4,%WarningLev
el%,3,50|%WarningLevel0%,60|%WarningLevel1%,70|%WarningLevel2%,80|%WarningLevel3%,90|%
WarningLevel4%
MACHINE\SYSTEM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod,4,%ScreenSaverGracePeriod%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta,4,%
DynamicBacklogGrowthDelta%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog,4,%Enabl
eDynamicBacklog%,0
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog,4,%Mini
mumDynamicBacklog%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog,4,%Maxi
mumDynamicBacklog%,3,10000|%MaximumDynamicBacklog0%,15000|%MaximumDynamicBacklog1%,200
```

```
00|%MaximumDynamicBacklog2%,40000|%MaximumDynamicBacklog3%,80000|%MaximumDynamicBacklo
g4%,160000|%MaximumDynamicBacklog5%
MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\SafeDllSearchMode,4,%SafeDllSe
archMode%,0
```

9. Wechseln Sie zum Ende des Bereichs **[Strings]** und kopieren den folgenden Text in die Datei:

```
;============================== MSS Settings==============================
EnableICMPRedirect = "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF
generated routes"
SynAttackProtect = "MSS: (SynAttackProtect) Syn attack protection level(protects
against DoS)"
SynAttackProtect0 = "No additional protection, use default settings"
SynAttackProtect1 = "Connections time out sooner if a SYN attack is detected"
EnableDeadGWDetect = "MSS: (EnableDeadGWDetect) Allow automatic detection of
dead network gateways (could lead to DoS)"
EnablePMTUDiscovery = "MSS: (EnablePMTUDiscovery ) Allow automatic detection of MTU
size (possible DoS by an attacker using a small MTU)"
KeepAliveTime = "MSS: How often keep-alive packets are sent in milliseconds"
KeepAliveTime0 ="150000 or 2.5 minutes"
KeepAliveTime1 ="300000 or 5 minutes (recommended)"
KeepAliveTime2 ="600000 or 10 minutes"
KeepAliveTime3 ="1200000 or 20 minutes"
KeepAliveTime4 ="2400000 or 40 minutes"
KeepAliveTime5 ="3600000 or 1 hour"
KeepAliveTime6 ="7200000 or 2 hours (default value)"
DisableIPSourceRouting = "MSS: (DisableIPSourceRouting) IP source routing protection
level (protects against packet spoofing)"
DisableIPSourceRouting0 = "No additional protection, source routed packets are
allowed"
DisableIPSourceRouting1 = "Medium, source routed packets ignored when IP forwarding is
enabled"
DisableIPSourceRouting2 = "Highest protection, source routing is completely disabled"
TcpMaxConnectResponseRetransmissions = "MSS:(TcpMaxConnectResponseRetransmissions)
SYN-ACK retransmissions when a connection request is not acknowledged"
TcpMaxConnectResponseRetransmissions0 = "No retransmission, half-open connections
dropped after 3 seconds"
TcpMaxConnectResponseRetransmissions1 = "3 seconds, half-open connections dropped
after 9 seconds"
TcpMaxConnectResponseRetransmissions2 = "3 & 6 seconds, half-open connections dropped
after 21 seconds"
TcpMaxConnectResponseRetransmissions3 = "3, 6, & 9 seconds, half-open connections
dropped after 45 seconds"
TcpMaxDataRetransmissions = "MSS: (TcpMaxDataRetransmissions) How many times
unacknowledged data is retransmitted (3 recommended, 5 is default)"
PerformRouterDiscovery = "MSS: (PerformRouterDiscovery) Allow IRDP to detect and
configure Default Gateway addresses (could lead to DoS)"
TCPMaxPortsExhausted = "MSS: (TCPMaxPortsExhausted) How many dropped connect requests
to initiate SYN attack protection (5 is recommended)"
NoNameReleaseOnDemand = "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore
NetBIOS name release requests except from WINS servers"
NtfsDisable8dot3NameCreation = "MSS: Enable the computer to stop generating 8.3 style
filenames"
NoDriveTypeAutoRun = "MSS: Disable Autorun for all drives"
NoDriveTypeAutoRun0 = "Null, allow Autorun"
NoDriveTypeAutoRun1 = "255, disable Autorun for all drives"
WarningLevel = "MSS: Percentage threshold for the security event log at which the
system will generate a warning"
WarningLevel0 = "50%"
WarningLevel1 = "60%"
WarningLevel2 = "70%"
WarningLevel3 = "80%"
WarningLevel4 = "90%"
```

```
ScreenSaverGracePeriod = "MSS: The time in seconds before the screen saver grace
period expires (0 recommended)"
DynamicBacklogGrowthDelta = "MSS: (AFD DynamicBacklogGrowthDelta) Number of
connections to create when additional connections are necessary for Winsock
applications (10 recommended)"
EnableDynamicBacklog = "MSS: (AFD EnableDynamicBacklog) Enable dynamic backlog for
Winsock applications (recommended)"
MinimumDynamicBacklog = "MSS: (AFD MinimumDynamicBacklog) Minimum number of free
connections for Winsock applications (20 recommended for systems under attack, 10
otherwise)"
MaximumDynamicBacklog = "MSS: (AFD MaximumDynamicBacklog) Maximum number of 'quasi-
free' connections for Winsock applications"
MaximumDynamicBacklog0 = "10000"
MaximumDynamicBacklog1 = "15000"
MaximumDynamicBacklog2 = "20000 (recommended)"
MaximumDynamicBacklog3 = "40000"
MaximumDynamicBacklog4 = "80000"
MaximumDynamicBacklog5 = "160000"
SafeDllSearchMode = "MSS: Enable Safe DLL search mode (recommended)"
```

10. Speichen und schließen Sie die Datei.
11. Öffnen Sie die Kommandozeile und tippen Sie das Kommando **regsvr32 scecli.dll**, damit die SCE.dll erneut registriert wird.

Sicherheitsüberlegungen in Bezug auf Netzwerkangriffe

Damit mögliche Denial of Service (DoS) Angriffe verhindert werden, sollten Sie Ihren Computer immer mit den neusten Sicherheitsupdates aktualisieren. Gerade das TCP/IP-Protokoll (Transmission Control Protocol/Internet Protocol) und der TCP/IP-Protokollstapel von Windows® Server 2003™ sollten immer durch die neusten Informationen und Programme sicher gegenüber Angriffen konfiguriert sein. Die Standardimplementierung des TCP/IP-Protokolls ist vornehmlich auf Leistung und standard TCP/IP Verkehr ausgelegt. Sollten Sie den Computer direkt an das Internet anschließen, empfiehlt Microsoft die TCP/IP Implementierung gegen so genannte DoS-Angriffe zu sichern.

DoS-Angriffe, die über das TCP/IP Protokoll gelenkt werden, lassen sich in zwei Kategorien einteilen: Angriffe, die eine enorme Anzahl von Systemressourcen benutzen, zum Beispiel durch das Öffnen vieler TCP-Verbindungen, und Angriffe, die durch Manipulation von TCP-Paketen dazu führen können, dass sich das Netzwerk fehlerhaft verhält. Die folgenden Registrierungseinträge helfen dabei, den TCP/IP Protokollstapel des Betriebssystems zu sichern. DoS-Angriffe sind zum Beispiel das Fluten eines Webservers mit Verbindungsanfragen oder einem Ping. Dadurch werden die Ressourcen des Webservers blockiert, und dieser kann nicht mehr auf normale Anfragen antworten. Auch andere Teile eines Netzwerkes, wie Router und Server, können durch zu viele Pakete langsamer werden, oder gar nicht mehr auf Verbindungsanfragen reagieren. DoS-Angriffe sind aus diesem Grunde schwer zu verhindern. Folgende Registrierungseinstellungen sollen helfen, Angriffe zu verhindern und den TCP/IP Protokollstapel zu sichern.

Diese Registrierungsschlüssel finden Sie unter dem folgenden Pfad:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

Tabelle 10.1: TCP/IP Parameter, die zur Registrierung von Windows® Server 2003 hinzugefügt werden

Name des Unterschlüssels	Format	Empfohlene Werte (Dezimal)
EnableICMPRedirect	DWORD	0
SynAttackProtect	DWORD	1
EnableDeadGWDetect	DWORD	0
EnablePMTUDiscovery	DWORD	0

KeepAliveTime	DWORD	300000
DisableIPSourceRouting	DWORD	2
TcpMaxConnectResponseRetransmissions	DWORD	2
TcpMaxDataRetransmissions	DWORD	3
PerformRouterDiscovery	DWORD	0
TCPMaxPortsExhausted	DWORD	5

EnableICMPredirect: Erlaubt ICMP Umleitungen (redirects), die von OSPF generierten Routinginformationen zu überschreiben

Dieser Eintrag wird unter dem Namen **MSS: Allow ICMP redirects to override OSPF generated routes** angezeigt. Die Internet Control Message Protocol (ICMP) -Umleitung führt dazu, dass der TCP/IP Protokollstapel Routen verwirft bzw. überschreibt, die durch OSPF generiert wurden.

Sicherheitslücken

Das oben beschriebene Verhalten entspricht den Erwartungen, birgt aber Gefahren. Und zwar, weil für die ICMP-Umleitungen als Zeitüberschreitung ein Wert von 10 Minuten gesetzt ist. Während dieser Zeit entsteht ein Black Hole im betreffenden Netzwerk, da die Routinginformationen verloren sind und neu aufgebaut werden müssen.

Gegenmaßnahme

Konfigurieren Sie die Einstellung **MSS: Allow ICMP redirects to override OSPF generated routes** auf **Aktiviert**.

Die möglichen Werte für diesen Registrierungsschlüssel sind:

- Aktiviert
- Deaktiviert
- Nicht definiert

Potenzielle Auswirkung

Sollte der Routing und RAS Dienst (RRAS) eingerichtet sein, und der Server einen autonomen Grenzrouter eines Systems (Autonomous System Boundary Router (ASBR)) bilden, werden die verbundenen Netzwerkschnittstellen, bzw. die entsprechenden Routen, nicht korrekt importiert. Da ein OSPF Router nicht als ASBR benutzt werden kann, werden durch den Import der Routen der Netzwerkschnittstellen durch OSPF fehlerhafte Routen und Routingtabellen generiert, was zu nicht absehbaren Folgen führt.

SynAttackProtect: Schutz vor Synchronisationsangriffen (schützt vor DoS Angriffen)

Dieser Eintrag wird unter dem Namen **MSS: Syn attack protection level (protects against DoS)** angezeigt. Er bewirkt, dass das TCP-Protokoll die Übermittlung von Bestätigungspaketen (SYN-ACKs) mit einem kürzeren Wert für die Zeitüberschreitung versieht. Dadurch wird ein Angriff besser abgewehrt, der nur Verbindungsinitialisierungen durchführt, aber keine dieser Verbindungen dann nutzt, da die Verbindungsinitialisierungen bei Nichtbenutzung sofort wieder verworfen werden.

Sicherheitslücken

Bei einem sogenannten SYN-Angriff sendet der Angreifer permanent Verbindungsinitialisierungspakete (SYN-Pakete) an den Server, der dann auf weitere Daten wartet. Dies hat zu Folge, dass der Server eine Vielzahl an halboffenen Verbindungen vorhält, bis keine Ressourcen mehr zur Verfügung stehen, um weitere Verbindungen zu initialisieren. Der Server kann somit nicht mehr antworten.

Gegenmaßnahme

Tragen Sie den Wert **Connections time out sooner if a SYN attack is detected** ein.

Mögliche Werte für diese Einstellung sind:

- Connections time – out more quickly if a SYN attack is detected
- No additional protection, use default settings
- Nicht definiert

Potenzielle Auswirkung

TCP Verbindungsanfragen haben bei einem SYN-Angriff geringe Gültigkeitsdauer. Beachten Sie dabei, dass andere TCP-Einstellungen, wie zum Beispiel die TCP-Fenstergröße und die Initial Round Trip Time (RTT), Probleme bereiten können.

EnableDeadGWDetect: Erlauben der automatischen Erkennung von nicht funktionierenden Gateways (kann zu einem DoS-Zustand führen)

Der Eintrag **MSS: Allow automatic detection of dead network gateways** im SCE regelt dieses Verhalten. Falls mehrere Verbindungen Probleme mit dem bisherigen Gateway haben, kann das TCP-Protokoll andere Gateways nutzen.

Sicherheitslücken

Ein Angreifer könnte den Server dazu bringen, eine falsche Gateway-Adresse zu benutzen.

Gegenmaßnahmen

MSS: Allow automatic detection of dead network gateways sollte auf **Deaktiviert** stehen.

Mögliche Werte für diese Einstellung sind:

- Aktiviert
- Deaktiviert
- Nicht definiert

Potenzielle Auswirkung

Bei deaktivierter Erkennung verhindern Sie, dass Windows nicht funktionierende Gateways erkennt und automatisch andere Gateways benutzt.

EnablePMTUDiscovery: Automatische Erkennung der MTU Größe (möglicher DoS Angriff mit kleiner MTU)

Der Name diese Einstellung lautet **MSS: Allow automatic detection of MTU size (possible DoS by an attacker using a small MTU)**. Wenn die automatische Erkennung angeschaltet ist, versucht der TCP/IP Protokollstapel die maximale TCP-Paketgröße oder die Maximum Transmission Unit (MTU) für die Kommunikation mit einem Remoterechner zu benutzen.

Sicherheitslücken

Wenn Sie die automatische Erkennung nicht abschalten, könnte ein Angreifer die MTU auf einen sehr kleinen Wert setzen, so dass der Server die Pakete für eine Übertragung in viele kleine Fragmente aufteilen müsste.

Gegenmaßnahmen

Setzen Sie den Wert **MSS: Allow automatic detection of MTU size (possible DoS by an attacker using a small MTU)** auf **deaktiviert**.

Mögliche Werte für diese Einstellung sind:

- Aktiviert
- Deaktiviert
- Nicht definiert

Potenzielle Auswirkung

Bei eingeschalteter **EnablePMTUDiscovery** wird bei jedem Verbindungsaufbau die größte TCP-Paketgröße auf dem Weg zu einem entfernten Rechner als Maximalgröße der Pakete festgelegt.

Das TCP-Protokoll verhindert die Fragmentierung einzelner Pakete über Router hinweg. Eine Fragmentierung hat allgemein einen negativen Effekt auf den Durchsatz von TCP-Paketen. Bei abgeschalteter Erkennung wird eine MTU von 576 Bytes für alle Verbindungen benutzt, sofern es sich um Verbindungen zu Rechnern außerhalb des lokalen Netzes handelt.

KeepAliveTime: Wie lange (in Millisekunden) Keep-Alive Pakete gesendet werden (300.000 sind empfohlen)

Der Eintrag wird unter dem Namen **MSS: How often keep alive packets are sent in milliseconds (300,000 is recommended)** angezeigt. Dieser Wert kontrolliert, wie lange das TCP-Protokoll versucht eine bestehende Verbindung durch die so genannten Keep-Alive Pakete aufrechtzuerhalten. Solange der entfernte Rechner erreichbar ist, bestätigt dieser jedes dieser Pakete.

Sicherheitslücken

Angreifer können durch diese Einstellung und durch den Aufbau sehr vieler Verbindungen die Erreichbarkeit des Computers einschränken. Typischer DoS-Angriff.

Gegenmaßnahmen

Konfigurieren Sie den Eintrag: **MSS: How often keep alive packets are sent in milliseconds (300,000 is recommended)** auf **300000 oder 5 Minuten**.

Die möglichen Werte dieser Einstellung sind:

- 150000 or 2.5 minutes
- 300000 or 5 minutes
- 600000 or 10 minutes
- 1200000 or 20 minutes
- 2400000 or 40 minutes
- 3600000 or 1 hour
- 7200000 or 2 hours (default)
- Nicht definiert

Potenzielle Auswirkung

Keep-Alive Pakete werden normalerweise nicht gesendet. Erst durch den Einsatz der Sicherheitseinstellungen können Werte für die Verbindungen gesetzt werden. Dies gibt Ihnen die Möglichkeit, die Standardeinstellung von 2 Stunden auf 5 Minuten zu verringern. Damit werden allerdings auch inaktive Verbindungen deutlich schneller abgebaut.

DisableIPSourceRouting: IP source routing protection level (Schutz gegen Paketmanipulation)

Der angezeigte Name dieser Einstellung lautet **MSS: IP source routing protection level (protects against packet spoofing).** Dieser Mechanismus erlaubt es dem Sender eines IP-Pakets die Route, die dieses Datagramm durch das Netzwerk nehmen soll, festzulegen.

Sicherheitslücken

Ein Angreifer kann so genannte Source-Routed-Pakete benutzen, um seine Identität und seinen Aufenthaltsort zu verschleiern. Source-Routing erlaubt einem Computer die Route, die ein Paket nehmen soll, zu bestimmen.

Gegenmaßnahmen

Konfigurieren Sie die Einstellung auf **Highest protection, source routing is completely disabled.**

Folgende Werte sind für die Einstellung möglich:

- **No additional protection, source routed packets are allowed**
- **Medium, source routed packets ignored when IP forwarding is enabled**
- **Highest protection, source routing is completely disabled**
- **Nicht definiert**

Potenzielle Auswirkung

Die entsprechenden Pakete werden verworfen.

TcpMaxConnectResponseRetransmissions: Erneutes Senden eines SYN-ACK Paketes, wenn eine Verbindungsanfrage nicht bestätigt wird.

Diese Einstellung wird als **MSS: SYN-ACK retransmissions when a connection request is not acknowledged** angezeigt. Sie bestimmt die Anzahl der Versuche, die das TCP-Protokoll durch weitere SYN-Packete vornimmt, bevor der Verbindungsversuch abgebrochen wird. Der Zeitraum bis zur erneuten Übertragung wird nach jedem weiteren Versuch verdoppelt. Der Standardwert liegt bei 3 Sekunden.

Sicherheitslücken

Während eines so genannten SYN-Flood-Angriffs schickt der Angreifer permanent SYN-Pakete an den Server und lässt diese halboffenen Verbindungen dann ungenutzt. Der Server ist nach einiger Zeit nicht mehr in der Lage, echte Verbindungsanfragen entgegenzunehmen, da die entsprechenden Ressourcen verbraucht sind.

Gegenmaßnahmen

Konfigurieren Sie die Einstellung auf **3 seconds, half-open connections dropped after 9 seconds**.

Folgende Werte sind für die Einstellung möglich:

- **No retransmission, half-open connections dropped after 3 seconds (0)**
- **3 seconds, half-open connections dropped after 9 seconds (1)**
- **3 & 6 seconds, half-open connections dropped after 21 seconds (2)**
- **3, 6, & 9 seconds, half-open connections dropped after 45 seconds (3)**
- **Nicht definiert**

Potenzielle Auswirkung

Wird ein Wert größer oder gleich **2** gewählt, so nutzt der TCP/IP Protokollstapel interne Mechanismen, um sich vor einem SYN-Angriff zu schützen. Eine Einstellung die kleiner **2** ist, hält den TCP/IP Protokollstapel davon ab, alle Registrierungsschlüssel bezüglich des Schutzes vor einem SYN-Angriff zu lesen. Dieser Parameter verkürzt also die Zeit für halboffene TCP-Verbindungen. Bei einem schweren Angriff kann der Wert auf **1,** oder sogar auf **0** gesetzt werden. Ist der Wert **0**, wird kein erneutes Senden erfolgen. Somit muss bei jeder Verbindungsanfrage innerhalb von 3 Sekunden eine Verbindung aufgebaut werden. Für weit entfernte Clients könnte diese Zeitbegrenzung nicht ausreichend sein, und Verbindungsversuche können fehlschlagen.

TcpMaxDataRetransmissions: Wie oft unbestätigte Daten erneut gesendet werden (3 empfohlen, 5 Standard)

Diese Einstellung wird unter dem Namen **MSS: How many times unacknowledged data is retransmitted (3 recommended, 5 is default)** angezeigt. Sie kontrolliert die Anzahl der vor dem Verbindungsabbruch erneut gesendeten TCP-Daten (non-connect Segment). Die Zeitüberschreitung wird bei jeder erneuten Übermittlung verdoppelt. Der Zähler wird zurückgesetzt, wenn eine Verbindung wieder aufgenommen wird. Die Zeitüberschreitung wird dynamisch anhand der gemessenen Round trip time (RTT) der jeweiligen Verbindung bestimmt.

Sicherheitslücken

Während eines so genannten SYN-Flood-Angriffs schickt der Angreifer permanent SYN-Pakete an den Server und lässt diese halboffenen Verbindungen dann ungenutzt. Der Server ist nach einiger Zeit nicht mehr in der Lage, neue Verbindungsanfragen entgegenzunehmen, da die entsprechenden Ressourcen verbraucht sind.

Gegenmaßnahmen

Konfigurieren Sie die Einstellung auf den Wert **3**.

Folgende Werte sind für die Einstellung möglich:

- **Eine benutzerdefinierte Zahl**
- **Nicht definiert**

Potenzielle Auswirkung

Wenn Pakete an die IP-Schicht gegeben werden, startet das TCP Protokoll einen Timer für die erneute Übertragung. Solange keine Bestätigung des Empfängers für ein Segment zurückkommt, wird das Segment entsprechend dem konfigurierten Wert erneut versandt.

PerformRouterDiscovery: Erlaubnis für IRDP die Standardgatewayadresse zu konfigurieren (Vorsicht DoS-Angriffe)

Diese Einstellung wird unter dem Namen **MSS: Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)** angezeigt. Sie wird benutzt, um die Funktion des Internet Router Discovery Protokolls (Internet Router Discovery Protocol (RDP) zu aktivieren oder zu deaktivieren. Das IRDP ermöglicht dem System, automatisch eine Standardgateway-Adresse zu konfigurieren.

Sicherheitslücken

Ein Angreifer kann, wenn er bereits Zugriff auf einem Computer im Netzwerksegment hat, andere Systeme dadurch täuschen, dass der bereits angegriffene Rechner sich im betroffenen Netzwerk als Router zu erkennen gibt. Alle Computer, bei denen IRDP aktiviert ist, werden dann versuchen sämtliche Daten über diesen Computer zu schicken.

Gegenmaßnahmen

Deaktivieren Sie die Einstellung.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht definiert**

Potenzielle Auswirkung

Durch das Deaktivieren wird verhindert, dass der Standardgateway automatisch konfiguriert wird.

TCPMaxPortsExhausted: Wie viele verworfene Verbindungsinitialisierungen den Schutz gegen SYN-Angriffe anschalten (5 empfohlen).

Die Einstellung wird unter dem Namen **MSS: How many dropped connect requests to initiate SYN attack protection (5 is recommended)** angezeigt. Sie kontrolliert den Schutz gegen SYN-Angriffe, und wird aktiv, wenn die Anzahl der Verbindungsanfragen (connection requests) den vorgegebenen Wert übersteigt.

Sicherheitslücken

Während eines so genannten SYN-Flood-Angriffs schickt der Angreifer permanent SYN-Pakete an den Server und lässt diese halboffenen Verbindungen dann ungenutzt. Der Server ist nach einiger Zeit nicht mehr in der Lage, neue Verbindungsanfragen entgegenzunehmen, da die entsprechenden Ressourcen verbraucht sind.

Gegenmaßnahmen

Konfigurieren Sie die Einstellung auf den Wert **5**.

Die möglichen Werte für die Einstellung sind:

- Benutzerdefinierte Anzahl
- Nicht definiert

Potenzielle Auswirkung

Dieser Eintrag sollte keine Auswirkungen auf Serversysteme haben, solange diese in normaler Art und Weise benutzt werden.

AFD.SYS Einstellungen

Bei Windows® Socket-Anwendungen, wie zum Beispiel dem File Transfer Protokoll (FTP) Server oder dem Webserver, werden die Verbindungsversuche durch die Datei *Afd.sys* gesteuert. Diese Datei wurde modifiziert, damit eine bessere Unterstützung für viele Verbindungen im halboffenen Zustand gewährleistet wird, ohne ordnungsgemäßen Clients den Zugriff zu verbieten. Dies wurde dadurch erreicht, dass Administratoren den Wert der Verbindungsanzahl und die damit verbundenen Ressourcen einstellen können. Die *Afd.sys* Datei von Windows® Server 2003 unterstützt vier Registrierungswerte die dieses Verhalten kontrollieren.

Diese Registrierungsschlüssel finden Sie unter dem folgenden Pfad:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters

Tabelle 20.2: Afd.sys Einstellungen, die in der Registrierung von Windows® Server 2003 hinzugekommen sind

Name des Unterschlüssels	Format	Empfohlene Werte (Dezimal)
DynamicBacklogGrowthDelta	DWORD	10
EnableDynamicBacklog	DWORD	1
MinimumDynamicBacklog	DWORD	20
MaximumDynamicBacklog	DWORD	20000

DynamicBacklogGrowthDelta: (AFD DynamicBacklogGrowthDelta) Verbindungsanzahl die erstellt werden soll, wenn zusätzliche Verbindungen notwendig sind für Winsock-Anwendungen (empfohlen 10)

Diese Einstellung wird unter dem Namen **MSS: (AFD DynamicBacklogGrowthDelta) Number of connections to create when additional connections are necessary for Winsock applications (10 recommended)** angezeigt. Sie kontrolliert die Anzahl der freien Verbindungen, die erstellt werden, wenn zusätzliche Verbindungen notwendig sind. Gehen Sie mit diesem Wert vorsichtig um, da eine große Zahl dazu führen kann, dass viele freie Verbindungen vorgehalten werden, obwohl sie tatsächlich nie gebraucht werden.

Sicherheitslücken

Während eines so genannten SYN-Flood-Angriffs schickt der Angreifer permanent SYN-Pakete an den Server und lässt diese halb offenen Verbindungen dann ungenutzt. Der Server ist nach einiger Zeit nicht mehr in der Lage, neue Verbindungsanfragen entgegenzunehmen, da die entsprechenden Ressourcen verbraucht sind.

Gegenmaßnahmen

Setzen Sie die Einstellung auf den Wert **10**.

Die folgenden Werte sind für die Einstellung möglich:

- **Benutzerdefinierte Anzahl**
- **Nicht definiert**

Potenzielle Auswirkung

Ein zu großer Wert kann dazu führen, dass zu viele Systemressourcen für diese Verbindungen verbraucht werden, obwohl sie nicht benötigt werden. Dies kann zu einer verschlechterten Leistung des Servers, oder einem DoS-Zustand führen.

EnableDynamicBacklog: (AFD EnableDynamicBacklog) Aktivierung des dynamischen Vorhaltens von freien Verbindungen (Backlog) für Winsock-Anwendungen (empfohlen)

Diese Einstellung wird unter dem Namen **MSS: (AFD EnableDynamicBacklog) Enable dynamic backlog for Winsock applications (recommended)** angezeigt. Sie ist ein globaler Schalter für alle Winsock-Anwendungen.

Sicherheitslücken

Socket-Anwendungen sind empfänglich für DoS-Angriffe.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Die mögliche Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht definiert**

Potenzielle Auswirkung

Die Auswirkungen sollten gering sein, solange Sie die anderen hier empfohlenen Einstellungen übernehmen. Allerdings kann, wie bereits weiter oben erwähnt, ein hoher Wert dazu führen, dass der Server langsamer antwortet oder in einen DoS Zustand gerät.

MinimumDynamicBacklog: (AFD MinimumDynamicBacklog) Minimale Anzahl der freien Verbindungen für Winsock-Anwendungen (20 empfohlen bei einem Angriff, ansonsten 10)

Diese Einstellung wird unter dem Namen **MSS: (AFD MinimumDynamicBacklog) Minimum number of free connections for Winsock applications (20 recommended for systems under attack, 10 otherwise)** angezeigt. Sie bestimmt die Anzahl der freien Verbindungen, die vom Server vorgehalten werden. Wird die Anzahl unterschritten, beginnt ein Thread neue zusätzliche Verbindungen zur Verfügung zu stellen. Der Wert sollte nicht zu groß gewählt werden, da beim Unterschreiten des Schwellenwertes sofort neue Ressourcen des Servers verbraucht werden. Zu große Werte führen unweigerlich zu verminderter Leistung.

Sicherheitslücken

Socket-Anwendungen sind empfänglich für DoS-Angriffe.

Gegenmaßnahmen

Setzen Sie den Wert der Einstellung auf **10**.

Die folgenden Werte sind für die Einstellung möglich:

- **Eine benutzerdefinierte Zahl**
- **Nicht definiert**

Potenzielle Auswirkung

Ist der Wert zu hoch, kann dies dazu führen, dass Systemressourcen verschwendet werden. So kann es zu Leistungseinbußen oder einem DoS-Zustand kommen.

MaximumDynamicBacklog: (AFD MaximumDynamicBacklog) Maximale Anzahl von ’quasi freien’ Verbindungen für Winsock-Anwendungen

Diese Einstellung wird unter dem Namen **MSS: (AFD MaximumDynamicBacklog) Maximum number of 'quasi-free' connections for Winsock applications** angezeigt. Sie beschränkt die Anzahl der freien Verbindungen auf dem Server. „Quasi frei“ bedeutet in diesem Zusammenhang alle freien und halb verbundenen (SYN_RECEIVED) Verbindungen. Durch diese Einstellung wird kein Versuch unternommen zusätzliche Verbindungen vorzuhalten, wenn deren Anzahl die maximale Anzahl übersteigen.

Sicherheitslücken

Socket-Anwendungen sind empfänglich für DoS-Angriffe.

Gegenmaßnahmen

Der vorgeschlagene Wert für ein gerade angegriffenes System ist arbeitsspeicherabhängig. Dabei sollte der Wert 5000 pro 32 MB RAM des Servers nicht überschritten werden, um eine vollständige Auslastung des nicht ausgelagerten Bereichs während eines Angriffs zu vermeiden. Als guter Einstieg empfiehlt sich ein System zu Testzwecken mit dem Wert **2000** zu konfigurieren.

Die folgenden Werte sind für die Einstellung möglich:

- **10000**
- **15000**
- **20000**
- **40000**
- **80000**
- **160000**
- **Nicht definiert**

Potenzielle Auswirkung

Ein zu hoher Wert kann zur Verschwendung von Systemressourcen und zu Leistungseinbußen führen.

Configure NetBIOS Name Release Security: (NoNameReleaseOnDemand) Erlaubt dem Computer NetBIOS Namensanfragen zu ignorieren, solange diese nicht vom WINS Servers stammen

Diese Einstellung wird unter dem Namen **MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers** angezeigt. NetBIOS über TCP/IP ist ein Netzwerkprotokoll, dass eine einfach Möglichkeit bietet, NetBIOS-Namen, die auf Windowssystemen an die IP-Adresse eines Rechners gebunden werden, aufzulösen. Der Wert bestimmt, ob ein Computer seinen NetBIOS-Namen auf einfache Anfragen hin angibt oder nicht.

Sie finden die Einstellung unter dem folgenden Pfad gesetzt:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters

Tabelle 30.3: Neuer Registrierungsschlüssel zum Schutz gegen einfache NetBIOS-Namensabfragen

Name des Unterschlüssels	Format	Empfohlene Werte (Dezimal)
NoNameReleaseOnDemand	DWORD	1

Sicherheitslücken

Das NetBIOS über TCP/IP (NetBT) Protokoll verwendet keine Authentifizierung. Deshalb ist dieses Protokoll anfällig gegenüber Angriffen (spoofing). Dabei wird beispielsweise dem System vorgegaukelt, dass eine Anfrage von einer anderen Person gestellt wird. Durch die Informationen, die ein Angreifer somit bekommt, könnte dieser versuchen den gleichen NetBIOS-Namen in dem Netzwerk zu registrieren. Durch diesen Namenskonflikt kann es vorkommen, dass der angegriffene

Computer nicht mehr auf Anfragen aus dem Netz reagiert, weil ein doppelt auftauchender NetBIOS-Name nicht vorgesehen ist und somit zu Komplikationen führt.

Das Ergebnis könnte eine unterbrochene Verbindung sein. Diese verhindert, dass die Netzwerkumgebung, die Domänenanmeldungen, das Send-Kommando oder die NetBIOS-Namensauflösung vom angegriffenen System aus genutzt werden können.

Mehr Informationen zu diesem Thema erhalten Sie im Microsoft Knowledge Base-Artikel Q269239 “MS00-047:NetBIOS Vulnerability May Cause Duplicate Name on the Network Conflicts” (englischsprachig).

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht definiert**

Alternativ dazu können Sie auch die Nutzung des Windows Internet Namens Servers (WINS) in Ihrem Netzwerk abschalten. Allerdings sollten Sie vorher überprüfen, ob keine Anwendung mehr von diesem abhängig ist, bzw. ob alle Domänenanmeldungen auch ausschließlich über DNS funktionieren. Dieser Austausch der Namensdienste sollte allgemein eine langfristige Strategie darstellen. Viele Anwendungen sind vom WINS-Server abhängig. Diese Abhängigkeit kann nicht immer schnell durch eine neue Version der Software ausgeglichen werden, da eine solche Umstellung sorgfältig geplant werden sollte.

Wenn Sie diese Gegenmaßnahme nicht ergreifen können und Sie die NetBIOS-Namensauflösung gewährleisten wollen, können Sie mit Hilfe eines zusätzlichen Schritts die Namen durch die *LMHOSTS* Datei zur Verfügung stellen. Mehr Informationen finden Sie in der *LMHOSTS* Datei, oder in dem Knowledge Base-Artikel Q269239 (englischsprachig).

> **Anmerkung:** Bei dieser Vorgehensweise müssen Sie mit einem erheblichen Konfigurationsaufwand rechnen. Deshalb empfiehlt Microsoft die Nutzung eines WINS-Servers gegenüber einer statischen Datei.

Potenzielle Auswirkung

Ein Angreifer kann eine Anfrage schicken, die den Computer auffordert seinen NetBIOS-Namen nicht weiter zu benutzen. Wie bei jeder Änderung hat auch diese Auswirkungen auf die verwendeten Anwendungen. Microsoft empfiehlt, diese Einstellungen erst auf einem Testsystem einzurichten und zu beobachten, bevor sie in der Produktivumgebung eingesetzt wird.

Disable Auto Generation of 8.3 File Names: Deaktivieren Sie die Generierung der 8.3 Namen für Dateien.

Diese Einstellung wird unter dem Namen **MSS: Enable the computer to stop generating 8.3 style filenames** angezeigt. Windows Server 2003 unterstützt das 8.3-Namensformat wegen der Abwärtskompatibilität von 16-Bit-Anwendungen. Diese Namenskonvention erlaubt Dateinamen mit maximal acht Zeichen Länge.

Sie finden die Einstellungen unter dem Pfad:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation

Tabelle 10.4: Deaktivieren Sie die Generierung der 8.3 Namen für Dateien

Name des Unterschlüssels	Format	Empfohlene Werte (Dezimal)
NtfsDisable8dot3NameCreation	DWORD	1

Sicherheitslücken

Ein Angreifer benötigt nur acht Zeichen um eine Datei anzusprechen, obwohl der Dateiname zum Beispiel 20 Zeichen lang ist. Eine Datei, die den Namen *Diesisteinlangerdateiname.doc* trägt, kann auch über die 8.3 Unterstützung als *Diesis~1.doc* angesprochen werden. Sollten Sie keine 16-Bit Anwendungen nutzen, können Sie diese Funktion bedenkenlos abschalten. Die Deaktivierung dieser Funktion führt bei einem NTFS Dateisystem zur Leistungsverbesserung bei der Verzeichnisanzeige.

Angreifer könnten diese kurzen Dateinamen verwenden, um damit auf Daten oder Anwendungen zuzugreifen, deren lange Dateinamen schwierig zu erraten und zu finden wären. Ein Angreifer, der Zugriff auf das Dateisystem erlangt, kann Daten sichten oder Anwendungen ausführen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht definiert**

Mögliche Auswirkungen

Noch im Einsatz befindliche 16-Bit-Anwendungen haben keine Möglichkeit mehr, auf Dateien mit längeren Namen als dem 8.3 Format zuzugreifen.

> **Anmerkung:** Sollten Sie diese Einstellung vornehmen, werden bereits bestehende kurze Dateinamen bestehen bleiben. Damit schon existierende 8.3 Namen ebenfalls entfernt werden, müssen Sie die Dateien an eine andere Stelle kopieren und an den ursprünglichen Orten löschen. Anschließend kopieren Sie die Dateien zurück.

Disable Autorun: Deaktivieren der Autostart Funktion für alle Laufwerke

Diese Einstellung wird unter dem Namen **MSS: Disable Autorun for all drives** angezeigt. Die Autostart Funktion liest beim Einlegen eines Mediums vom entsprechenden Laufwerk. Das Ergebnis kann sein, dass Installationsprogramme oder Filme automatisch gestartet werden.

Sie finden die Einstellung unter dem folgenden Pfad:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

Tabelle 10.5: Deaktivieren der Autostart Funktion aller Laufwerke

Name des Unterschlüssels	Format	Empfohlene Werte (Dezimal)
NoDriveTypeAutoRun	DWORD	0xFF

Alternativ dazu können Sie unter dem folgenden Pfad mit dem Eintrag **1** die Autostart-Funktion der CDROM/ DVD-Laufwerke deaktivieren:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom

Tabelle 10.6: Deaktivieren der Autostart Funktion aller CDROM/ DVD Laufwerke

Name des Unterschlüssels	Format	Empfohlene Werte (Dezimal)
AutoRun	DWORD	0

Sicherheitslücken

Um eine mögliche Gefahr durch ein bösartiges Programm zu verhindern, wird die Autostart-Funktion aller Laufwerke mit der Richtlinie deaktiviert.

Ein Angreifer mit direktem Zugang zu einem System könnte ein spezielle CD/ DVD in den Computer einlegen und dann die Schadroutinen und Programme automatisch starten lassen. Mit diesen kann ein Angreifer dann weitere Programme aufrufen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf den Wert **255, disable Autorun for all drives**.

Mögliche Werte für diese Einstellung sind:

- **Null, allow Autorun**
- **255, disable Autorun for all drives**
- **Nicht definiert**

Mögliche Auswirkungen

Die Autostartfunktion wird nicht mehr verwendet. CDs oder DVDs werden beim Einlegen nicht mehr automatisch abgespielt.

Make Screensaver Password Protection Immediate: Die Zeit in Sekunden, bevor der Bildschirmschoner den Computer auch wirklich sperrt (0 empfohlen)

Diese Einstellung wird unter dem Namen **MSS: The time in seconds before the screen saver grace period expires (0 recommended)** angezeigt. Windows wartet zwischen dem Zeitpunkt, an dem der Bildschirmschoner gestartet wird, und dem Moment in dem die Computerkonsole wirklich gesperrt ist, einen Moment ab (funktioniert nur bei angeschaltetem Kennwortschutz für den Bildschirmschoner).

Sie finden die Einstellung unter dem folgenden Pfad:
HKEY_LOCAL_MACHINE\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Tabelle 10.7: Einstellung für die sofortige Aktivierung des Bildschirmschonerpassworts

Name des Unterschlüssels	Format	Empfohlene Werte (Dezimal)
ScreenSaverGracePeriod	String	0

Sicherheitslücken

Der Zeitraum, bis der Bildschirmschoner anläuft und die Passwortkontrolle aktiviert wird, beträgt fünf Sekunden. Während dieser Zeit könnte ein Angreifer durch ein Büro laufen und Zugriff auf das System erlangen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf den Wert **0** ein.

Die möglichen Werte für diese Einstellung sind:

- **Eine benutzerdefinierte Zahl zwischen 0 und 255**
- **Nicht definiert**

Mögliche Auswirkungen

Benutzer müssen ihre Passwörter immer dann eingeben, wenn der Bildschirmschoner gestartet wurde.

Security Log Near Capacity Warning: Prozentangabe des Schwellenwertes, bei dem das Sicherheitsprotokoll eine Warnmeldung generiert.

Diese Einstellung wird unter dem Namen **MSS: Percentage threshold for the security event log at which the system will generate a warning** angezeigt. Der Windows Server 2003 und das Servicepack 3 von Windows 2000 enthalten eine neue Funktion. Diese generiert eine Warnmeldung, sollte das Sicherheitsprotokoll einen vom Benutzer definierten Schwellenwert überschreiten. Wenn Sie die Einstellung zum Beispiel auf **90** setzen, erscheint bei Erreichen dieses Wertes in der Ereignisanzeige ein Ereignis mit der ID 523 und dem Text „Das Sicherheitsprotokoll ist zu 90 Prozent voll“.

> **Anmerkung:** Diese Einstellung zeigt keine Wirkung, wenn das Sicherheitsprotokoll so eingestellt ist, dass die Einträge bei Bedarf überschrieben werden.

Sie finden die Einstellung unter dem folgenden Pfad:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security

Tabelle 10.8: Einstellung für die Warnschwelle des Sicherheitsprotokolls

Name des Unterschlüssels	Format	Empfohlene Werte (Dezimal)
WarningLevel	DWORD	0

Sicherheitslücken

Sollte sich das Sicherheitsprotokoll füllen, und der Computer wurde nicht so konfiguriert, dass er beim Erreichen der Sicherheitsprotokolldateigröße herunterfahren soll, können keine weiteren Protokolleinträge vorgenommen werden. Sollte der Server zum Herunterfahren beim Erreichen der Sicherheitsprotokolldateigröße konfiguriert sein, könnte es zu einem DoS-Zustand kommen.

Gegenmaßnahmen

Setzen Sie die Einstellung auf den Wert **90**.

Die möglichen Werte für diese Einstellung sind:

- **50%**
- **60%**
- **70%**
- **80%**
- **90%**
- **Nicht definiert**

Mögliche Auswirkungen

Sollte das Sicherheitsprotokoll über 90% gefüllt sein, wird ein Eintrag in der Ereignisanzeige erzeugt. Diese Einstellung funktioniert nicht, wenn die Sicherheitseinträge bei Bedarf überschrieben werden.

Enable Safe DLL Search Order: Aktivieren der sicheren Suchabfolge für DLL Dateien

Diese Einstellung wird unter dem Namen **MSS: Enable Safe DLL search mode (recommended)** angezeigt. Die Suche nach DLLs (dynamic link libraries) kann auf zwei Arten durchgeführt werden:

- Zuerst die DLLs in den festgelegten Systempfaden und dann die im aktuell benutzten Ordner.
- Zuerst die DLLs im aktuellen Ordner und dann die in den Systemordnern.

Sie finden die Einstellung über den folgenden Pfad:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager

Tabelle 10.8: Aktivieren der sicheren Suchabfolge für DLL Dateien

Name des Unterschlüssels	Format	Empfohlene Werte (Dezimal)
SafeDllSearchMode	DWORD	0

Sicherheitslücken

Sollte ein Benutzer unwissentlich schädlichen Programmcode ausführen, und dieser Code dann mit modifizierten System DLLs weiterarbeiten, könnte sich der entstehende Schaden schnell vergrößern.

Gegenmaßnahmen

Setzen Sie die Einstellung auf **Aktiviert**.

Die möglichen Werte für diese Einstellung sind:

- **Aktiviert**
- **Deaktiviert**
- **Nicht definiert**

Potenzielle Auswirkung

Anwendungen werden gezwungen, die gewählte Suchreihenfolge für DLL Dateien einzuhalten. Systempfade werden dabei zuerst durchsucht. Bei Anwendungen, die ihre eigenen DLLs benötigen, kann es zu Leistungs- und Stabilitätsproblemen kommen.

11

Zusätzliche Sicherheitseinstellungen für Mitgliedsserver

Obwohl Sie die meisten Gegenmaßnahmen dieses Handbuchs über Gruppenrichtlinien einrichten können, gibt es zusätzliche Einstellungen, bei denen dies nicht möglich ist. Dieses Kapitel beschreibt einige weitere Gegenmaßnahmen, wie zum Beispiel die Einrichtung von Sicherheitskonten. Es erklärt außerdem deren Hintergrund, enthält zusätzliche Quellenangaben und eine Konfigurationsanweisung für die Verwendung von IP-Sicherheitsfiltern (IP Sec) als eine effektive Gegenmaßnahme gegen Netzwerkangriffe.

Sichern von Benutzerkonten

Microsoft® Windows Server 2003 hat eine gewisse Anzahl von eingebauten Benutzerkonten, die Sie nicht löschen, aber umbenennen können. Zwei sehr bekannte Benutzerkonten unter Windows Server 2003 sind das **Gast** und das **Administrator** Konto.

Sicherheitslücken

Das **Gastk**onto wird durch die Standardinstallation auf einem Mitgliedsserver oder einem Domänenkontroller deaktiviert. Ändern Sie diese Einstellung nicht. Benennen Sie das Konto **Administrator** um, und ändern Sie dessen Beschreibung, um einen Angriff auf bekannte Konten zu verhindern.

Viele Variationen von Angriffen nutzen gerade dieses bekannte Benutzerkonto **Administrator** um in den Server einzubrechen. Der Schutz durch die Umbenennung hat allerdings in den letzten Jahren abgenommen, da viele Angriffe und Tools versuchen über den Security Identifier (SID) des Administratorkontos einzubrechen. Die SID ist die Nummer, die jeden Benutzer, jede Gruppe, jedes Computerkonto und jede Anmeldesitzung in einem Netzwerk eindeutig definiert. Es ist nicht möglich die SID eines eingebauten Benutzerkontos zu verändern.

Gegenmaßnahmen

Benennen Sie das Benutzerkonto **Administrator** um, und vergeben Sie ein langes und mit Sonderzeichen versehenes Kennwort.

Anmerkung: Der Name des Administrators kann mit Hilfe einer Gruppenrichtlinie umbenannt werden. Die standardmäßig vorhandenen Gruppenrichtlinien des Microsoft Windows Server 2003-Sicherheitshandbuchs verändern den Namen nicht, damit Sie einen individuellen Namen vergeben können. Die Umbenennung des Administrators durch eine Gruppenrichtlinie erreichen Sie durch den Eintrag **Konten: Administrator umbenennen** innerhalb der Gruppenrichtlinie an folgender Stelle:
Computerkonfiguration\Windows-Einstellungen\SicherheitsSettings\Lokale Richtlinie\Sicherheitsoptionen
Idealerweise sollten verschiedene Kennwörter auf den einzelnen Servern eingerichtet werden, doch das lässt sich in der Praxis häufig nicht durchsetzen. Protokollieren Sie alle Änderungen, und verwahren Sie diese an einem sicheren Ort auf. Sollte auf allen Servern eines Netzwerks der gleiche Name verwendet werden, kann ein Angreifer mit dem bekannt werden dieses Kennwortes sofort alle Rechner übernehmen.

Potenzielle Auswirkung

Benutzer und Administratoren, die für bestimmte Systeme verantwortlich sind, müssen jederzeit über die jeweiligen verwendeten Namen auf den einzelnen Systemen informiert sein. Benutzer, die im Rahmen ihrer Aufgaben ein lokales Administratorenkonto benötigen, müssen Zugang zu den geänderten Namen und dem verwendeten Passwort haben.

NTFS

Das NTFS Dateisystem unterstützt die Zugriffskontrolle mit Hilfe von so genannten “Access Control Lists” (ACLs). Bei diesem Dateisystem besteht auch die Möglichkeit, mit Verschlüsselung (EFS) auf Datei- und Ordnerebene zu arbeiten. Zugriffskontrolle und Verschlüsselung wird bei den Dateisystemen FAT und FAT32 nicht unterstützt. FAT32 ist eine Erweiterung des ursprünglichen FAT Dateisystems.

Sicherheitslücken

Dateien, die nicht durch ACLs geschützt werden können, sind für nicht berechtigte Benutzer einfach anzuzeigen, zu ändern oder zu löschen. Dabei spielt es keine Rolle, ob die Benutzer lokal oder über ein Netzwerk Zugriff auf diese Dateien erhalten. ACLs helfen an dieser Stelle die Dateien zu schützen. Verschlüsselung von Dateien erzielt ein höheres Maß an Sicherheit, gerade wenn es sich um Dateien handelt, die nur von einem einzelnen Benutzer verwendet werden.

Gegenmaßnahmen

Formatieren sie alle Partitionen auf den Servern mit dem NTFS Dateisystem. Konvertieren Sie bereits bestehende FAT Partitionen ohne Datenverlust in NTFS Partitionen mit dem **convert.exe** Tool. Beachten sie allerdings dabei, dass bei dieser Konvertierung die ACLs auf der umgewandelten Partition für alle Dateien und Ordner auf **Jeder: Vollzugriff** eingestellt werden.

Für den Windows Server 2003 und Windows XP basierende Systeme wenden Sie die folgenden Sicherheitsvorlagen an, um die Standardzugriffsrechte (ACLs) zu setzen:

- Für Arbeitsstationen: %windir%\inf\defltwk.inf
- Für Server: %windir%\inf\defltsv.inf
- Für Domänenkontroller: %windir%\inf\defltdc.inf

Anweisungen zur lokalen Anwendung von Sicherheitsvorlagen finden Sie in *Kapitel 11, Absicherung von öffentlichen Hosts*, des *Windows Server 2003 Sicherheitshandbuchs*.

> **Anmerkung:** Die Domänenkontroller-Sicherheitseinstellungen werden beim Heraufstufen eines Servers zum Domänenkontroller automatisch gesetzt.

Potenzielle Auswirkung

Es gibt keine negativen Auswirkungen.

> **Anmerkung:** Richtig und sauber implementierte NTFS Berechtigungen werden Ihre Daten vor Offenlegung und Veränderung schützen. Allerdings sollte auch der direkte Zugriff auf Systeme bedacht werden. Ist ein Angreifer in der Lage, den Computer direkt zu bedienen, so kann dieser mit Hilfe einer startfähigen CD-ROM oder einer Diskette ein anderes Betriebssystem verwenden, um auf die Daten zuzugreifen. Auch beim Diebstahl von Festplatten kann ein Angreifer diese dann in andere Systeme einhängen und auf die Daten zugreifen. Hat der Angreifer die Kontrolle über das jeweilige Speichermedium erlangt, ist es schwer die Daten noch zu schützen.

Dies ist ein fundamentales Problem in der heutigen Computertechnologie, dass auch bei anderen Dateisystemen anderer Betriebssystemhersteller vorkommt. Hat ein Angreifer den physikalischen Zugriff auf die Platte, können die NTFS-Berechtigungen und andere Schutzmechanismen leicht umgangen werden. Microsoft die folgenden Sicherheitsmaßnahmen:

- Benutzen Sie SYSKEY mit einem offline Passwort, damit nicht berechtigte Personen davon abgehalten werden, das Windows Betriebssystem zu benutzen.
- Setzen Sie EFS ein, damit Benutzerdaten verschlüsselt werden können. Weisen Sie die Benutzer an, Domänenbenutzerkonten zu verwenden, und bestimmen Sie den Domänenadministrator mittels einer Gruppenrichtlinie zum Wiederherstellungsagenten.
- Setzen Sie im Basic Input/Output System (BIOS) ein Passwort, damit verhindert wird, dass nicht berechtigte Benutzer den Computer starten können.
- Stellen Sie im BIOS das Starten von CD-ROM-Laufwerken und Diskettenlaufwerken aus. Dies hält Angreifer davon ab, den Computer mit deren eigenem Betriebssystem zu starten.

Trennung von Daten und Anwendungen

Es ist lange bekannt, dass die Trennung von Daten, Anwendungen und Betriebssystemdateien auf jeweilige spezielle Speichermedien die Leistung des Systems erhöhen kann. Ein weiterer Grund für diese Trennung ist der Schutz vor Angriffen, die über Ordnergrenzen hinweg Schaden anrichten (Directory-Traversal-Angriffe).

Sicherheitslücken

Allgemein gibt es zwei Klassen von Sicherheitslücken durch Anwendungen, Daten und Protokolldateien, sofern sich diese auf der gleichen Partition wie das Betriebssystem befinden. Eine potentielle Möglichkeit ist, dass ein Benutzer unwissentlich oder vorsätzlich durch Anwendungsdaten oder Einträge in Protokolldateien die Partition füllt, so dass dieses Laufwerk keinen freien Platz mehr hat. Dies kann auch durch kopieren über das Netz erreicht werden.

Die zweite Möglichkeit ist das Ausnutzen von so genannten “Traversal Exploits”, bei denen ein Angreifer durch Schwachstellen in einem Netzwerkdienst durch die Verzeichnisstruktur wechseln kann, um zum Systemordner zu gelangen. Ist ein Angreifer dort angelangt, ist es ihm möglich weitere Programme aufzurufen.

Es gibt mittlerweile tausend oder mehr Variationen dieser Angriffe. Die IIS waren in den letzten Jahren sehr verwundbar gegenüber solchen Angriffen. Beispiele hierfür sind NIMDA oder CODE RED, die einen Pufferüberlauf ausnutzten, damit die Angreifer anschließend im Dateisystem Programme wie die *cmd.exe* aufrufen konnten.

Deshalb ist es wichtig, wann immer es möglich ist Webdokumente, Anwendungen, Daten und Anwendungsprotokolldateien in einer separaten Partition abzulegen.

Gegenmaßnahmen

Wenn möglich, legen Sie Webdokumente, Anwendungen, Daten und Anwendungsprotokolldateien auf eine andere Partition als die Betriebssystemdateien.

Potenzielle Auswirkung

Für Unternehmen, die Server immer in der gleichen Weise aufsetzen, sollte der Einfluss gering sein. Bei Organisationen, die Server nicht immer gleich aufsetzen, ist der Aufwand höher, weil die Administratoren erst herausfinden müssen, wie die einzelnen Systeme eingerichtet wurden.

Konfigurieren des SNMP Community Namens

Das Simple Network Management Protokoll (SNMP) ist das Standard-Netzwerkmanagementprotokoll, welches häufig in TCP/IP-Netzwerken eingesetzt wird. SNMP stellt Managementmethoden für Netzwerkknoten (Nodes), die zentral von einer Maschine aus gemanagt werden, zur Verfügung. Netzwerkknoten können Arbeitstationen, Server, Router, Netzwerkbrücken oder Hubs oder anderer Netzwerkkomponenten sein, die eine SNMP Unterstützung bieten. Das Managementprotokoll arbeitet mit zwei Teilen: Mit der Managementkomponente und dem Agenten. Auf der zentralen Maschine wird die Managementkomponente ausgeführt und auf den Netzwerkknoten (Nodes) die Agentenkomponente.

Der SNMP Dienst nutzt eine sehr einfache Form der Sicherheit, indem so genannte Community-Namen für die gegenseitigen Authentifizierungspakete verwendet werden. Sie können die SNMP-Kommunikation einschränken, indem Sie dem Agenten mitteilen, an welche Community er nur Meldungen verschicken darf. Hierbei ist auch die Angabe mehrere Communities möglich. Diese Namen werden dann für die Authentifizierungsnachrichten im SNMP-Protokoll benutzt und stellen ein sehr einfaches System der Absicherung da. Obwohl ein Rechner in mehreren Communities Mitglied sein kann, wird ein Agent nur SNMP-Nachrichten von dem Manager akzeptieren, der aus den eingestellten Communities stammt. Es gibt keinen direkten Zusammenhang zwischen einem Community-Namen und einem Domänennamen oder Arbeitsgruppennamen, da diese alle unabhängig voneinander eingestellt werden. Es ist Ihre Aufgabe, bei der Installation des SNMP-Dienstes den Namen so zu wählen, dass er nicht einfach zu erraten ist.

Sicherheitslücken

Das SNMP Protokoll ist in seinem Aufbau kaum auf Sicherheit ausgelegt. Die größte Sicherheitslücke im SNMP Protokoll ist sicherlich, dass nahezu alle Hersteller von Komponenten einen Standardnamen für die Community einrichten. Diese Standardnamen sind bekannt. Bei Microsoft wird zum Beispiel der Name *public* als Standardname verwendet.

Eine zweite Sicherheitslücke ist schwieriger zu bekämpfen. Die SNMP-Kommunikation sendet den Community-Namen immer im Klartext. Daraus ergibt sich eine einfache Möglichkeit bei der Übertragung von SNMP-Nachrichten den Community-Namen zu sehen, da er nicht verschlüsselt oder gehasht wird. Gegenmaßnahmen sind möglich, indem Sie den IP Verkehr zwischen den Servern komplett verschlüsseln. Diese Gegenmaßnahme würde den Rahmen dieses Dokuments allerdings sprengen.

Gegenmaßnahmen

Konfigurieren Sie den SNMP-Community-Namen mit Leseberechtigung auf allen Systemen und einem zufällig generierten alphanumerischen Namen.

So konfigurieren Sie den Community-Namen:

1. In der Dienstesteuerung doppelklicken Sie den **SNMP-Dienst**.
2. Klicken Sie auf die Registerkarte **Sicherheit** des SNMP-Dienstes.
3. Wählen Sie den Eintrag **public** aus der Liste der **Akzeptierten Communitynamen** aus.
4. Klicken Sie auf die **Bearbeiten** Schaltfläche und schreiben Sie einen neuen Namen in das erscheinende **Communityname** Dialogfenster.
5. Klicken Sie **Ok** um die Dialogfenster zu schließen.

Lassen Sie den Schreibzugriff via SNMP-Protokoll deaktiviert.

Anmerkung: Der Community-Name wird in der Registrierung als ein DWORD Wert mit dem Eintrag 4 abgelegt. Somit ist es möglich diese Prozedur mittels Skripten zu automatisieren. Sie können auch durch den Eintrag in die Sicherheitsvorlage das Ganze mit einer

Gruppenrichtlinie domänenweit einstellen. Der Wert wird unter folgendem Pfad eingetragen: *HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities*

Mögliche Auswirkungen

Jede Managementsoftware, die den Community-Namen verwendet, muss entsprechend umkonfiguriert werden.

Deaktivierung von NetBIOS und SMB auf Netzwerkschnittstellen, die mit öffentlichen Netzen verbunden sind.

Dieser Abschnitt befasst sich mit Empfehlungen für Server, die in Netzwerken stehen, die nicht vollständig kontrolliert werden können. Dies können Webserver im Internet oder Mailserver sein, die über einen Zugang zum Internet verfügen. Diese Server werden auch als öffentlich erreichbare Hosts bezeichnet. Sollten Sie verantwortlich für einen solchen Server sein, implementieren Sie die folgenden Änderungen. Testen Sie diese Einstellungen sorgfältig und versichern Sie sich, dass Sie die Änderungen verstehen. Die Deaktivierung des NetBIOS Systems bringt beispielsweise Veränderungen mit sich, die sich dann auf die Verwaltung des Servers auswirken werden.

Sicherheitslücken

Die Deaktivierung des Server Message Block (SMB)-Protokolls und des NetBIOS über TCP/IP Protokolls sichert einen öffentlichen Rechner dadurch, dass die Angriffsfläche deutlich verkleinert wird. Allerdings werden auch die Möglichkeiten des Servermanagements eingeschränkt. So ist es dann nicht mehr möglich, auf freigegebene Ordner zuzugreifen. Aus diesem Grunde ist es sinnvoll, Einstellungen für Netzwerkverbindungen, die direkt mit dem Internet verbunden sind, vorzunehmen.

Gegenmaßnahmen

Deaktivierung von NetBIOS ist nicht ausreichend um eine SMB Kommunikation zu verhindern, da SMB bei fehlenden NetBIOS Ports versuchen wird, den TCP Port 445 zu benutzen. Dieser wird auch als SMB Direct Host, oder als Common Internet File System (CIFS) Port bezeichnet. Deshalb müssen beide separat abgeschaltet werden.

NetBIOS benutzt die folgenden Ports:

- UDP/137 (NetBIOS Name Service)
- UDP/138 (NetBIOS Datagramm Service)
- TCP/139 (NetBIOS Session Service)

SMB benutzt die folgenden Ports:

- TCP/139
- TCP/445

Auf Servern, die vom Internet aus erreichbar sind, sollten Sie die SMB-Unterstützung durch das Entfernen der **Datei- und Druckerfreigabe für Microsoft-Netzwerke** und des **Client für Microsoft-Netzwerke** ausschalten. Dies kann über die Einstellungen des **Internetprotokoll (TCP/IP)** in den **Netzwerkverbindungen** der jeweiligen Netzwerkverbindung konfiguriert werden.

Deaktivierung des SMB- Protokolls:

1. In der Systemsteuerung doppelklicken sie auf Netzwerkverbindungen.
2. Rechtsklick auf jede dem Internet zugewandte Verbindung und klicken Sie auf die Eigenschaften.
3. In dem Dialogfenster wählen Sie den Eintrag Client für Microsoft-Netzwerke aus und klicken auf Deinstallieren.
4. Folgen Sie den Deinstallationsanweisungen.
5. Wählen Sie den Eintrag Datei- und Druckerfreigabe für Microsoft-Netzwerke aus und klicken dann auf Deinstallieren.
6. Folgen Sie den Deinstallationsanweisungen.

So deaktivieren Sie NetBIOS über das TCP/IP Protokoll:

1. In der **Systemsteuerung** doppelklicken Sie auf **System**, dann auf die Registerkarte **Hardware** und schließlich auf die Schaltfläche **Gerätemanager**.
2. In der Menüleiste klicken Sie auf **Ansicht** und dann auf **Ausgeblendete Geräte anzeigen**.
3. Erweitern Sie die Ansicht für **Nicht-PnP-Treiber**.
4. Rechtsklick auf **NetBIOS über TCP/IP** und dann auf **Deaktivieren**.

Dieser Vorgang deaktiviert den Direct Host Listener auf TCP und UDP Port 445.

Anmerkung: Dieser Eingriff deaktiviert den *nbt.sys* Treiber. Darüber wird der NetBIOS Session Service (der auf Anfragen auf Port 139 reagiert) deaktiviert. Dieses schließt allerdings nicht das Abschalten der SMB-Unterstützung mit ein. Um die SMB-Unterstützung abzuschalten folgen Sie den weiter oben detailliert aufgeführten Schritten zum Thema *Deaktivierung des SMB-Protokolls*.

Mögliche Auswirkungen

Das System ist nicht mehr in der Lage, mittels SMB Daten auszutauschen. Dies schließt freigegebene Ordner und diverse Verwaltungswerkzeuge mit ein.

Konfiguration des Terminal Server Ports

Terminaldienste sind ein nützliches Werkzeug für Netzwerkadministratoren, weil es ihnen ermöglicht, auf entfernte Server und in Benutzersitzungen einzugreifen. Der Remote Desktop Client wird standardmäßig auf allen Windows Server 2003 und Windows XP Systemen installiert. Außerdem ist dieser Client auch auf der Installations-CD-ROM des Windows Servers 2003 enthalten, und es steht auf der Microsoft Webseite ein ActiveX® Client, der mit dem Internet Explorer oder der Microsoft Management-Konsole (MMC) zusammenarbeitet, zur Verfügung. Diese Tools sind auch bekannt als Terminal Services Advanced Client (TSAC).

Sicherheitslücken

Die Terminaldienste von Microsoft arbeiten standardmäßig auf dem TCP Port 3389. Alle Remotedesktop-Clients versuchen sich mit diesem Port zu verbinden. Obwohl sämtliche übertragenen Daten einer Sitzung verschlüsselt sind, versucht der Client nicht die Identität des Servers zu bestätigen. Ein Angreifer könnte durch Manipulation die Benutzer auf einen falschen Server leiten.

Gegenmaßnahmen

Ändern Sie den TCP Port, der von den Terminaldiensten benutzt wird, oder implementieren Sie eine IPSec-Richtlinie um eine gesicherte Verbindung mittels Authentification Header (AH) oder

Encapsulation Security Payload (ESP) im IPSec-Transportmodus (nicht IPSec-Tunnelmodus) zu verwenden. In einem solchen Szenario ist es erstrebenswert, den Terminalserver hinter einem VPN-Gateway zu positionieren, so dass entweder das Point to Point Tunnel-Protokoll (PPTP) oder aber das L2TP-Protokoll verwendet werden, um einen sicheren VPN-Tunnel für den Zugriff auf den Terminalserver zur Verfügung zu stellen.

Mehr Informationen zur Änderung des vom Terminalserver verwendeten Ports und des Remote Desktop Clients erhalten Sie im Microsoft Knowledge Base-Artikel *How to Change Terminal Server's Listening Port* unter http://support.microsoft.com/default.aspx?scid=187623 (englischsprachig). Der Artikel gibt eine Anleitung, wie der normale Desktopclient konfiguriert werden muss. Wenn Sie die Einstellungen für den Webclient ändern möchten, müssen Sie innerhalb der Webseite die folgende Zeile einfügen: MsRdpClient.RDPport = *xxx* - wobei *xxx* für den bevorzugten TCP Port steht. Mehr Informationen zur Benutzung des Clients in Verbindung mit dem Internet Explorer finden Sie im Artikel *Providing for RDP Client Security* unter http://msdn.microsoft.com/library/default.asp?url=/library/en-us/termserv/termserv/providing_for_rdp_client_security.asp (englischsprachig).

Mögliche Auswirkungen

Die Implementierung von IPSec mit AH wird kaum negativen Einfluss auf die Systemleistung haben. Für die IKE-Sicherheitsaushandlung (Internet Key Exchange) für den Aufbau einer sicheren Verbindung werden Vertrauensstellungen benötigt. Die IPSec-Richtlinie kann entweder so eingestellt werden, dass der gesamte Netzwerkverkehr zum Server verschlüsselt wird, oder dass nur Verbindungen zum Port 3389 geschützt werden. Die Vorgabe, nur noch mit IPSec auf Serverseite zu kommunizieren, hat zur Folge, dass Clients, die kein IPSec sprechen können oder keine Vertrauensstellungen mit dem Server unterhalten, mit diesem keine Verbindung aufbauen können. Mehr zum Thema finden Sie im nächsten Abschnitt über den Gebrauch von IPSec-Richtlinien zur Absicherung von TCP/IP-Netzwerkverkehr.

Das Ändern des Standard-Terminalserverports führt dazu, dass alle Clients mit diesem neuen Port konfiguriert werden müssen. Der TSAC-Client unterstützt in der momentanen Version diesen Portwechsel noch nicht.

Konfiguration der IPSec-Richtlinien

IPSec ist ein Tool, das dem Netzwerkadministrator die Möglichkeit gibt TCP/IP-Verkehr zu erlauben, zu verbieten oder Sicherheitsverhandlungen vorzuschreiben. Für die darüber liegenden Anwendungen ist diese Art der Verschlüsselung nicht sichtbar. Das Designziel für Windows 2000 war, eine Möglichkeit zu finden, den Netzwerkverkehr durch das IPSec-Protokoll mit dem AH-Format oder dem ESP-Format zu sichern. IPSec-Richtlinien arbeiten mit statischen TCP/IP-Filtern, auch Selektoren genannt, die notwendig sind, um die Sicherheit mit IKE aufzubauen. IKE wird auch als ISAKMP-Protokoll bezeichnet. Weitere Informationen zu IPSec finden sie in Kapitel 6, *Deploying IPSec*, des Dokuments *Windows Server 2003 Deployment Kit: Deploying Network Services* unter http://www.microsoft.com/downloads/ details.aspx?FamilyID=5098c84a-8a9b-4e0f-bb27-254f5bfdaaa1&DisplayLang=en (englischsprachig).

Sicherheitslücken

Obwohl viele Netzwerk-Sicherheitsstrategien ihr Hauptaugenmerk auf die Verhinderung von Angriffen von außerhalb legen, ist es besser, sicherheitsrelevante oder vertrauliche Informationen zusätzlich gegen interne Angriffe zu schützen. Diese könnten einen Angriff gegen Schwachstellen auf höheren Schichten ausnutzen, um an wichtige Informationen zu gelangen. Ein Angreifer könnte so genannte NetBT-Nullsitzungen benutzen, um an das Administratorpasswort zu gelangen (sollten andere Sicherheitseinstellungen ungenutzt oder fälschlicher Weise ausgeschaltet sein). Ein Angreifer benötigt nur eine Sicherheitslücke in einer Anwendung, um Zugriff zu erlangen und unter Umständen die Kontrolle über einen Computer zu übernehmen. Wie bereits ausgeführt, werden viele Daten bei der Übertragung im Netzwerk nicht geschützt. Einigen Angestellten oder Besuchern könnte es möglich sein, sich in ein Netzwerk einzuhängen und die übertragenen Daten mitzuschneiden und später zu analysieren. Firewalls zwischen dem internen Netz und dem externen Netzwerk bieten keinen Schutz

vor solchen Bedrohungen. Interne Firewalls können häufig keine Authentifizierung übernehmen, um die Clients und Server zu schützen. Sie können auch keine Sicherheit von einem zum anderen Computer gewährleisten (Ende-zu-Ende-Sicherheit).

Gegenmaßnahmen

IPSec-Filter erkennen TCP/IP-Verkehr anhand ihrer Quell- und Ziel-IP-Adresse, des IP-Protokolltyps und des TCP/UDP-Ports. Deshalb kann ein IPSec-Filter dabei helfen, den Inhalt und die Verbreitung von schädlichem Code in Form von Würmern und Viren durch das gezielte abblocken zu verhindern. Außerdem kann es für Angreifer schwierig werden eine entfernte Shell oder andere Angriffstools zu benutzen, um aus einer verwundbaren Anwendung heraus Zugriff auf den Rechner zu erhalten. Mehr Informationen zur Konfiguration von IPSec-Richtlinien unter Windows 2000 finden Sie im Knowledge Base-Artikeln Q813878, *How to Block Specific Network Protocols and Ports by Using IPSec*, unter http://support.microsoft.com/default.aspx?scid=813878 oder *Using IPSec to Lock Down a Server (Windows 2000)* unter http://www.microsoft.com/serviceproviders/columns/using_ipsec.asp (englischsprachig).

Dieses Whitepaper gibt eine Schritt-für-Schritt-Anleitung, wie unter Windows 2000 IPSec-Filter eingerichtet werden. Dies ist vergleichbar mit der hier beschriebenen Vorgehensweise. Allerdings muss unter Windows 2000 noch die Registrierungseinstellung **NoDefaultExempt** nachgetragen werden.

Windows Server 2003™ stellt ein Snap-In für die Managementkonsole zur Verfügung, mit dem die IPSec-Richtlinien eingestellt und verwaltet werden können. Dieses Snap-In ist dem von Windows 2000 und Windows XP sehr ähnlich. Mit Windows Server 2003 steht sowohl die grafische Variante eines Snap-Ins zur Verfügung, als auch das Kommandozeilentool **Netsh** mit dem IPSec-Richtlinien und die damit verbundenen Filterrichtlinien angezeigt werden können.

Der nächste Abschnitt beschreibt die folgenden Begriffe:

- **IP-Filterliste:** Beinhaltet Ports, Protokolle und Filterrichtung. Die Filterliste löst eine Aktion aus, wenn der Netzwerkverkehr einem Kriterium der Liste entspricht. Eine Liste kann viele verschiedene Filter haben.
- **Filteraktion:** Die Aktion die erfolgen soll, wenn der Netzwerkverkehr die Kriterien des Filters erfüllt.
- **Filter:** Eine Regel, die in der Filterliste mit einer Filteraktion verknüpft ist.
- **IPSec-Richtlinie:** Eine Sammlung von Filtern. Es kann immer nur eine Richtlinie sein.

Eine einfache Möglichkeit diese Informationen festzuhalten ist eine Netzwerkverkehrstabelle. Diese dient dazu, alle Basiseinstellungen der Serverrolle aufzuzeichnen. Darin sollten der Name der Regel, die Richtung des Netzwerkverkehrs, das Ziel der Kommunikation, die IP-Adresse der Schnittstelle, das Protokoll, der TCP-Port und die UDP-Ports enthalten sein. Ein Beispiel für eine solche Netzwerkverkehrstabelle sehen Sie weiter unten in diesem Abschnitt.

Bevor Sie beginnen IPSec-Richtlinien zu erstellen, sollten Sie ein gutes Verständnis für den Netzwerkwerkverkehr ihres Servers haben, damit der Server später auch noch ordnungsgemäß funktioniert. Fehler können dazu führen, dass bestimmte Anwendungen nicht mehr ausgeführt werden können, da die Kommunikation zu stark eingeschränkt wurde.

So erstellen Sie eine Netzwerkverkehrstabelle:

1. Bestimmen Sie die wichtigen Netzwerkdienste des Servers und erstellen Sie eine Regel.
2. Identifizieren Sie die Protokolle und Ports für die einzelnen Dienste. Dazu können Sie beispielsweise den Netzwerkmonitor benutzen, um in die übertragenen Pakete des Netzwerks hineinzuschauen. Auch das Kommandozeilentool **netstat** kann verwendet werden, damit Sie sich bestehende TCP/IP-Verbindungen und -Sitzungen anschauen können.
3. Dokumentieren Sie die IPSec-Regeln, die notwendig sind, um den benötigten Netzwerkverkehr zuzulassen.

Starten Sie mit dem Filter mit den meisten Einschränkungen. Öffnen Sie später je nach Bedarf zusätzliche Ports. Durch diese Maßnahme erreichen Sie ein sehr hohes Maß an Sicherheit. Dieser Prozess ist einfacher, wenn Sie eine Unterscheidung zwischen Server- und Clientdiensten vornehmen. Der Serverdienst sollte für jeden Dienst definiert sein, den die Maschine für andere Computer zur Verfügung stellt.

Tabelle 11.1: Beispielnetzwerkverkehrstabelle

Dienst	Protokoll	Quellport	Zielport	Quelladresse	Zieladresse	Aktion	Gespiegelt
HTTP Server	TCP	beliebig(e)	80	beliebige IP-Adresse	Eigene IP-Adresse	Zulassen	JA
HTTPS Server	TCP	beliebig(e)	443	beliebige IP-Adresse	Eigene IP-Adresse	Zulassen	JA
DNS Client	TCP	beliebig(e)	53	Eigene IP-Adresse	DNS Server	Zulassen	JA
Alles abblocken	beliebig	beliebig(e)	beliebig(e)	beliebige IP-Adresse	beliebige IP-Adresse	Abblocken	JA

Wie in der Tabelle zu erkennen ist, wird ein mit diesen Regeln ausgestatteter Server alle Client HTTP- und HTTPS-Anfragen von jeder Client IP-Adresse akzeptieren. Der Eintrag **Eigene IP-Adresse** wird durch den IPSec-Filter als alle IP-Adressen des Servers interpretiert. Alle Filter sind gespiegelt und ermöglichen somit eine Antwort an den Computer, der die Anfrage gestellt hat. Das bedeutet, dass jeder Client eine Anfrage an den Webserverport 80 (IIS) stellen kann und der Spiegel dafür Sorge trägt, dass vom Port 80 eine Antwort an den Client geschickt werden kann.

Benötigt der Server den DNS-Clientdienst, um eine Namensabfrage an einen DNS Server zu stellen, wird ein weiterer Eintrag notwendig. In diesem Beispiel ist der Filter in Zeile 3 (DNS Client) derjenige, der solche DNS-Abfragen erlaubt. Windows Server 2003 verwendet hier gegenüber Windows 2000 eine vereinfachte Darstellung. Bei Windows 2000 muss hier immer der Port direkt angegeben werden, während bei Windows Server 2003 logische Namen, wie DNS-Server oder WINS-Server angezeigt werden. Außerdem müssen unter Windows 2000 immer alle DNS-Server einzeln eingegeben werden. Beachten Sie, dass die Richtlinien, die mit Windows Servern 2003 erstellt wurden, nicht auf Computern angewendet werden sollten, die mit den Betriebssystemen Windows 2000 oder Windows XP ausgeführt werden.

Die letzte Regel, *alles abblocken*, demonstriert eine andere Filterverbesserung unter Windows Server 2003. Diese Regel wird von Windows 2000 oder Windows XP nicht unterstützt. Sie blockiert sowohl eingehende, als auch ausgehende Multicast-, Broadcast- und Unicast-Pakete, die von keinem der anderen Filter erfasst werden.

Bedenken Sie beim Einsatz einer solchen Richtlinie, dass die Computer nicht mit einem DHCP Server, einem Domänencontroller, einem WINS-Server, mit Zertifikatsrückruflisten (CRLs) oder mit Computern, die Server überwachen, kommunizieren können. Ferner wird diese Richtlinie einem Administrator nicht erlauben, eine Fernwartung mit MMC Snap-Ins basierend auf RPC durchzuführen. Auch die Remotedesktopclient Verbindung wird durch die Richtlinie fehlschlagen. Beachten Sie zusätzlich, dass der Beispiel-IIS-Server mit zwei Netzwerkkarten ausgerüstet ist - eine für den Internetverkehr und die andere für den Intranetverkehr - diese Richtlinie für beide Netzwerkkarten anwendet und somit keine Unterscheidung bei der Anwendung der Filterregeln treffen kann. Die Richtlinie muss auf Ihre Bedürfnisse angepasst sein, damit Ihre speziellen Anforderungen erfüllt werden. Netzwerkverkehr sollte für die Schnittstelle zum Intranet anders gefiltert werden, als für die Schnittstelle zum Internet.

Ist ein Clientdienst notwendig, für den keine Einschränkung bezüglich der Zielserver festgelegt werden kann, wird die Sicherheit durch IPSec-Filter deutlich verringert. Im nächsten Beispiel wurde eine Regel hinzugefügt, die es dem Administrator ermöglicht den Webbrowser zu benutzen, um Hilfe-, Informations- und Downloadseiten aus dem Internet abrufen zu können. Die Regel benötigt einen

gespiegelten ausgehenden, statischen Filter, der den Netzwerkverkehr für den TCP Zielport 80 erlaubt.

Tabelle 11.2: Beispielnetzwerkverkehrstabelle die das Browsen im Internet erlaubt

Dienst	Protokoll	Quellport	Zielport	Quelladresse	Zieladresse	Aktion	Gespiegelt
Eingehend ICMP Daten für TCP PMTU	ICMP	beliebig(e)	beliebig(e)	beliebige IP-Adresse	Eigene IP-Adresse	Zulassen	nein
Eingehend IIS Server HTTP: 80	TCP	beliebig(Eigene IP-Adresse)	80	beliebige IP-Adresse	Eigene IP-Adresse	Zulassen	ja
Eingehend IIS Server FTP: 21	TCP	beliebig(Eigene IP-Adresse)	21	beliebige IP-Adresse	Eigene IP-Adresse	Zulassen	ja
Eingehend Terminal Server	TCP	beliebig(Eigene IP-Adresse)	3389	beliebige IP-Adresse	Eigene IP-Adresse	Zulassen	ja
Ausgehend zum Domänenkontroller alles	beliebig	beliebig(Eigene IP-Adresse)	beliebig(e)	Eigene IP-Adresse	Domänenname	Zulassen	ja
Ausgehend DNS UDP/TCP	UDP	beliebig(Eigene IP-Adresse)	53	Eigene IP-Adresse	DNS	Zulassen	ja
Ausgehend DNS UDP/TCP	TCP	beliebig(Eigene IP-Adresse)	53	Eigene IP-Adresse	DNS	Zulassen	ja
Ausgehend WINS	UDP	137	137	Eigene IP-Adresse	WINS	Zulassen	ja
Ausgehend DHCP	UDP	68	67	Eigene IP-Adresse	DHCP	Zulassen	ja
Ausgehend HTTP: 80	TCP	beliebig(Eigene IP-Adresse)	80	Eigene IP-Adresse	beliebige IP-Adresse	Zulassen	ja
Alles Abblocken	beliebig	beliebig(Eigene IP-Adresse)	beliebig(e)	beliebige IP-Adresse	beliebige IP-Adresse	Abblocken	ja

Obwohl diese Regeln wie eine durchdachte und vernünftige Konfiguration aussehen, bieten sie keinen Schutz davor, dass ein Angreifer eine Verbindung von außen auf einen Port des Computers herstellt. Durch die Spiegelung der Regel werden die Pakete auch wieder zurück an den Angreifer geschickt. Damit kann also der Angreifer jeden offenen Port von außen ansprechen, allerdings sollte er als Quellport den Port 80 benutzen.

Eine Vielzahl von Möglichkeiten existiert, damit auch solche Angriffe abgewehrt werden.

- Benutzen Sie zusätzliche IPSec-Filterregeln, um auch solche Angriffe von Port 80 aus zu verhindern.
- Benutzen Sie eine Firewall oder einen Router, um eingehende Verbindungen von Quellport 80 zu blockieren, sofern nicht vorher eine ausgehende Verbindung auf diesen Port erfolgte.
- Zusätzlich zu der oben erwähnten IPSec-Richtlinie stellen Sie die ICF (Internet Connection Firewall) auf der externen Schnittstelle ein, um ein genauere Filterung für alle ausgehenden Pakete mit Hilfe der IPSec-Filter zu erreichen. Da ICF in Schichten oberhalb von IPSec arbeitet, muss dort ebenfalls der TCP Port 80 und 433 eingehend erlaubt sein.

Das folgende Beispiel benutzt zusätzliche IPSec-Filter, um Angriffe von Port 80 aus abzublocken. Das Kommandozeilentool **netstat –ano** wird benutzt, um bestimmen zu können, welche TCP Ports auf einem Server geöffnet sein müssen. Auf diese könnte sich ein Angreifer verbinden:

```
D:\>netstat –ano

Aktive Verbindungen

  Proto  Lokale Adresse          Remoteadresse          Status           PID
  TCP    0.0.0.0:135             0.0.0.0:0              ABHÖREN          944
  TCP    0.0.0.0:445             0.0.0.0:0              ABHÖREN          4
  TCP    0.0.0.0:1025            0.0.0.0:0              ABHÖREN          4
  TCP    0.0.0.0:1046            0.0.0.0:0              ABHÖREN          508
  TCP    172.17.1.44:139         0.0.0.0:0              ABHÖREN          4
  UDP    0.0.0.0:445             *:*                                     4
  UDP    0.0.0.0:500             *:*                                     508
  UDP    0.0.0.0:1026            *:*                                     816
  UDP    0.0.0.0:1029            *:*                                     508
  UDP    0.0.0.0:1051            *:*                                     452
  UDP    0.0.0.0:4500            *:*                                     508
  UDP    127.0.0.1:123           *:*                                     884
  UDP    127.0.0.1:123           *:*                                     884
  UDP    172.17.1.44:137         *:*                                     4
  UDP    172.17.1.44:138         *:*                                     4
```

Die nächste Regel definiert das Abblocken von speziellen Angriffen, die den TCP Quellport 25 benutzen, um sich auf offene Ports zu verbinden:

Tabelle 11.3: Beispiel-Netzwerkverkehrstabelle, die das Browsen im Internet erlaubt

Dienst	Protokoll	Quellport	Zielport	Quelladresse	Zieladresse	Aktion	Gespiegelt
Eingehend ICMP Daten für TCP PMTU	ICMP	beliebig(e)	beliebig(e)	beliebige IP-Adresse	Eigene IP-Adresse	Zulassen	nein
Eingehend IIS Server HTTP: 80	TCP	beliebig(e)	80	beliebige IP-Adresse	Eigene IP-Adresse	Zulassen	ja
Eingehend IIS Server FTP: 21	TCP	beliebig(e)	21	beliebige IP-Adresse	Eigene IP-Adresse	Zulassen	ja
Eingehend Terminal Server	TCP	beliebig(e)	3389	beliebige IP-Adresse	Eigene IP-Adresse	Zulassen	ja
Ausgehend zum Domänenkontroller alles	beliebig	beliebig(e)	beliebig(e)	Eigene IP-Adresse	Domänenname	Zulassen	ja
Ausgehend DNS UDP/TCP	UDP	beliebig(e)	53	Eigene IP-Adresse	DNS	Zulassen	ja
Ausgehend DNS UDP/TCP	TCP	beliebig(e)	53	Eigene IP-Adresse	DNS	Zulassen	ja
Ausgehend WINS	UDP	137	137	Eigene IP-Adresse	WINS	Zulassen	ja
Ausgehend DHCP	UDP	68	67	Eigene IP-Adresse	DHCP	Zulassen	ja
Ausgehend	TCP	beliebig(e)	80	Eigene IP-	beliebige IP-	Zulassen	ja

HTTP: 80				Adresse	Adresse		
Verhindern der Angriffe von Quellport 80	TCP	80	135	beliebige IP-Adresse	Eigene IP-Adresse	Abblocken	nein
Verhindern der Angriffe von Quellport 80	TCP	80	139	beliebige IP-Adresse	Eigene IP-Adresse	Abblocken	nein
Verhindern der Angriffe von Quellport 80	TCP	80	445	beliebige IP-Adresse	Eigene IP-Adresse	Abblocken	nein
Verhindern der Angriffe von Quellport 80	TCP	80	1025	beliebige IP-Adresse	Eigene IP-Adresse	Abblocken	nein
Verhindern der Angriffe von Quellport 80	TCP	80	1046	beliebige IP-Adresse	Eigene IP-Adresse	Abblocken	nein
Alles Abblocken	beliebig	beliebig(e)	beliebig(Eigene IP-Adresse)	beliebige IP-Adresse	beliebige IP-Adresse	Abblocken	ja

Dieses Beispiel verdeutlicht, wie das Abblocken von Angriffen von außen erreicht werden kann. Dabei wird sämtlicher Verkehr, der von Port 80 auf einen aktiven Port des Rechners eine Verbindung herstellen will, abgeblockt. Somit ist von außen mit Quellport 80 keine Verbindung auf die Ports möglich, die für RPC, NetBT und SMB (CIFS) benutzt werden.

Es ist wiederum möglich, diese IPSec-Richtlinien mittels Gruppenrichtlinie auf mehrere Computer zu verteilen. Sie müssen **Netsh** benutzen, wenn Sie dauerhafte Richtlinien setzen wollen. Die folgende Datei kann mit **Netsh** hierzu verwendet werden. Sie können die Einrichtung durch Eingabe von **Netsh –f <Dateiname>** automatisch ausführen lassen.

```
pushd ipsec dynamic

set config property=ipsecexempt value=3
set config property=bootmode value=stateful
set config property=bootexemptions value="ICMP:inbound UDP:67:68:inbound
TCP:0:3389:inbound"

popd
pushd ipsec static

set store persistent
delete all
add policy name="PERS:Safe startup" activatedefaultrule=no
add filterlist name="PERS:Any to Any all traffic"
add filter filterlist="PERS:Any to Any all traffic" srcaddr=Any dstaddr=Any
description="PERS:Any<->Any all traffic, includes inbound and outbound multicast and
broadcast"
add filteraction name="PERS:BLOCK" action=block

add rule name="PERS:rule1" policy="PERS:Safe startup" filterlist="PERS:Any to Any
all traffic" filteraction="PERS:BLOCK"

set policy name="PERS:Safe startup" assign=yes

set store local
```

```
delete policy name="Domain Member IIS Server Permit/Block Lockdown, with outbound
HTTP:80 Access"
delete filterlist name="Any to Me, all traffic"
delete filterlist name="Inbound ICMP for TCP PMTU"
delete filterlist name="Inbound IIS Server:HTTP:80"
delete filterlist name="Inbound IIS Server:FTP:21"
delete filterlist name="Inbound Terminal Server"
delete filterlist name="Me to Domain DCs all traffic, <date>"
delete filterlist name="Outbound WINS"
delete filterlist name="Outbound UDP/TCP DNS"
delete filterlist name="Outbound DHCP"
delete filterlist name="Outbound HTTP:80"
delete filterlist name="Mitigation from inbound src 80 attack"
delete filteraction name="BLOCK"
delete filteraction name="PERMIT"

add policy name="Domain Member IIS Server Permit/Block Lockdown, with outbound HTTP:80
Access" description="Allow inbound HTTP, HTTPS, Remote Desktop. Allow outbound
HTTP:80, DC, DNS, WINS access. Used with persistent Any-to-Any all traffic block for
secure computer startup" activatedefaultrule=no
add filteraction name="BLOCK" action=block
add filteraction name="PERMIT" action=permit

add filterlist name="Any to Me, all traffic" description="also includes me to any
outbound unicast, multicast, broadcast"
add filter filterlist="Any to Me, all traffic" srcaddr=Any dstaddr=Me mirrored=yes
protocol=Any description="Any<->Me, all traffic"
add rule name="Block all unicast" policy="Domain Member IIS Server Permit/Block
Lockdown, with outbound HTTP:80 Access" filterlist="Any to Me, all traffic"
filteraction="BLOCK"

add filterlist name="Inbound ICMP for TCP PMTU"
add filter filterlist="Inbound ICMP for TCP PMTU" srcaddr=Any dstaddr=Me
protocol=ICMP mirrored=no description="Any->me ICMP for TCP PMTU"
add rule name="Enable TCP PMTU" policy="Domain Member IIS Server Permit/Block
Lockdown, with outbound HTTP:80 Access" filterlist="Inbound ICMP for TCP PMTU"
filteraction="PERMIT"

add filterlist name="Inbound IIS Server:HTTP:80"
add filter filterlist="Inbound IIS Server:HTTP:80" srcaddr=Any dstaddr=Me
protocol=TCP srcport=0 dstport=80 mirrored=yes description="Any<->Me, TCP src Any,
dst 80, inbound web"
add rule name="IIS Web Server" policy="Domain Member IIS Server Permit/Block
Lockdown, with outbound HTTP:80 Access" filterlist="Inbound IIS Server:HTTP:80"
filteraction="PERMIT" activate=yes

add filterlist name="Inbound IIS Server:FTP:21"
add filter filterlist="Inbound IIS Server:FTP:21" srcaddr=Any dstaddr=Me
protocol=TCP srcport=0 dstport=21 mirrored=yes description="Any<->Me, TCP src Any,
dst 80, inbound web"
add rule name="IIS FTP Server" policy="Domain Member IIS Server Permit/Block
Lockdown, with outbound HTTP:80 Access" filterlist="Inbound IIS Server:FTP:21"
filteraction="PERMIT" activate=no

add filterlist name="Inbound Terminal Server"
add filter filterlist="Inbound Terminal Server" srcaddr=Any dstaddr=Me
protocol=TCP srcport=0 dstport=3389 mirrored=yes description="Any<->Me, TCP src
Any, dst 3389, inbound remote desktop"
add rule name="Terminal Server" policy="Domain Member IIS Server Permit/Block
Lockdown, with outbound HTTP:80 Access" filterlist="Inbound Terminal Server"
filteraction="PERMIT" activate=no

popd
```

```
pushd ipsec dynamic
add mmpolicy name="N/A"
add rule srcaddr=Me dstaddr=DNS mmpolicy="N/A" protocol=UDP srcport=0 dstport=53
conntype=all mirrored=yes actionoutbound=permit actioninbound=permit
popd

pushd ipsec static

set store local

add filterlist name="Me to Domain DCs all traffic, <insert date>"
add filter filterlist="Me to Domain DCs all traffic, <insert date>" srcaddr=Me
dstaddr=<insert domain name> mirrored=yes protocol=any description="me<->my DC,
all traffic"
add rule name="DC client" policy="Domain Member IIS Server Permit/Block Lockdown,
with outbound HTTP:80 Access" filterlist="Me to Domain DCs all traffic, <insert
date>" filteraction="PERMIT"

popd
pushd ipsec dynamic
delete rule srcaddr=Me dstaddr=DNS protocol=UDP srcport=0 dstport=53 mirrored=yes
conntype=all
delete mmpolicy name="N/A"
popd

pushd ipsec static
set store local

add filterlist name="Outbound DNS UDP/TCP" description="Outbound UDP and TCP to
DNS Servers only using dynamic filter for DNS servers based on IP config"
add filter filterlist="Outbound DNS UDP/TCP" srcaddr=Me dstaddr=DNS protocol=UDP
mirrored=yes srcport=0 dstport=53 description="me<->DNS UDP src any, dst 53"
add filter filterlist="Outbound DNS UDP/TCP" srcaddr=Me dstaddr=DNS protocol=TCP
mirrored=yes srcport=0 dstport=53 description="me<->DNS TCP src any, dst 53"
add rule name="DNS Client" policy="Domain Member IIS Server Permit/Block Lockdown,
with outbound HTTP:80 Access" filterlist="Outbound DNS UDP/TCP"
filteraction="PERMIT"

add filterlist name="Outbound WINS" description="Outbound UDP to WINS Servers only
using dynamic filter for WINS servers based on IP config"
add filter filterlist="Outbound WINS" srcaddr=Me dstaddr=WINS protocol=UDP
mirrored=yes srcport=137 dstport=137 description="me<->WINS Servers UDP src 137,
dst 137"
add rule name="WINS Client" policy="Domain Member IIS Server Permit/Block
Lockdown, with outbound HTTP:80 Access" filterlist="Outbound WINS"
filteraction="PERMIT"

add filterlist name="Outbound DHCP" description="Outbound DHCP to DHCP Servers
only using dynamic filter for DHCP servers based on IP config"
add filter filterlist="Outbound DHCP" srcaddr=Me dstaddr=DHCP protocol=UDP
mirrored=yes srcport=68 dstport=67 description="me<->DHCP UDP src 68, dst 67"
add rule name="DHCP Client" policy="Domain Member IIS Server Permit/Block
Lockdown, with outbound HTTP:80 Access" filterlist="Outbound DHCP"
filteraction="PERMIT"

add filterlist name="Outbound HTTP:80"
add filter filterlist="Outbound HTTP:80" srcaddr=Me dstaddr=Any protocol=TCP
mirrored=yes srcport=0 dstport=80 description="me<->Any TCP src any, dst 80"
add rule name="web client" policy="Domain Member IIS Server Permit/Block Lockdown,
with outbound HTTP:80 Access" filterlist="Outbound HTTP:80" filteraction="PERMIT"

add filterlist name="Mitigation from inbound src 80 attack"
add filter filterlist="Mitigation from inbound src 80 attack" srcaddr=Any
```

```
dstaddr=Me description="Any->me TCP src 80, dst 135" protocol=TCP mirrored=no
srcport=80 dstport=135
add filter filterlist="Mitigation from inbound src 80 attack" srcaddr=Any
dstaddr=Me description="Any->me TCP src 80, dst 139" protocol=TCP mirrored=no
srcport=80 dstport=139
add filter filterlist="Mitigation from inbound src 80 attack" srcaddr=Any
dstaddr=Me description="Any->me TCP src 80, dst 445" protocol=TCP mirrored=no
srcport=80 dstport=445
add filter filterlist="Mitigation from inbound src 80 attack" srcaddr=Any
dstaddr=Me description="Any->me TCP src 80, dst 1025" protocol=TCP mirrored=no
srcport=80 dstport=1025
add filter filterlist="Mitigation from inbound src 80 attack" srcaddr=Any
dstaddr=Me description="Any->me TCP src 80, dst 1046" protocol=TCP mirrored=no
srcport=80 dstport=1046
add rule name="mitigate web client" policy="Domain Member IIS Server Permit/Block
Lockdown, with outbound HTTP:80 Access" filterlist="Mitigation from inbound src 80
attack" filteraction="BLOCK"

set policy name="Domain Member IIS Server Permit/Block Lockdown, with outbound
HTTP:80 Access" assign=no

popd

exit
```

Der letzte Schritt wäre die Zuweisung dieser Richtlinie mittels des MMC Snap-Ins IP-Sicherheitsrichtlinienverwaltung. Nach diesem Schritt benötigt der IPSec-Treiber einen Neustart, damit die Änderungen auch übernommen werden und wirksam sind.

IPSec-Schutz für Netzwerkverkehr aushandeln

Die Integration des IKE-Protokolls in die IPSec-Filter erlaubt den richtlinienbasierten, automatisierten Einsatz der IPSec-Verschlüsselung für den Unicast IP-Verkehr, der den IPSec-Filterregeln entspricht. Durch IPSec geschützte Pakete können Sie entweder das AH-Format, oder das ESP-Format mit verschiedenen Sicherheitsoptionen nutzen. IPSec-Richtlinien schützen den Netzwerkverkehr auf folgende Arten:

- Schutz in tiefen Protokollschichten gegen Angriffe. IPSec ist ein ausgereiftes State of the Art-Sicherheitsprotokoll, welches durch die IETF (Internet Engineering Task Force) entwickelt wurde. Es erlaubt Ihnen eine zusätzliche Schicht der Verteidigung für jegliche IP-Kommunikation zu verwenden, die einen verbesserten Schutz bietet. Deshalb kann IPSec dabei helfen, Schwächen höherer Protokolle und Schichten auszugleichen. Als Beispiel könnte man den Dateiaustausch mit dem SMB Protokoll heranziehen, weil dies bei der Microsoft Active Directory Replikation, beim Dateiaustausch, beim Drucken und beim Verteilen von Gruppenrichtlinien eine wichtige Rolle spielt. SMB als solches gewährt keinen Schutz. Alle Daten, die innerhalb von SMB verschickt werden, sind für einen passiven Netzwerkbeobachter sichtbar. Einzig die Möglichkeit SMB-Kommunikation zu signieren besteht. Der Einsatz der Signierung ist in manchen Fällen allerdings nicht ratsam, da dann sämtlicher SMB-Verkehr signiert wird. IPSec kann eingesetzt werden, um den Verkehr mit einem speziellen Netzwerkziel oder mehrere Zielen zu schützen. Bisher wurden zwei Sicherheitslücken in Windows 2000 und Windows XP bezüglich SMB festgestellt. Allerdings gibt es bei Microsoft für diese bereits entsprechende Sicherheitsupdates. Mehr Informationen über die SMB-Sicherheitslücken und die entsprechenden Sicherheitsupdates für Windows 2000 und Windows XP finden Sie in der Microsoft Knowledge Base in den beiden Artikeln:
- Q329170, *MS02-070: Schwachstelle bei SMB-Signierung ermöglicht Änderung von Gruppenrichtlinie* http://support.microsoft.com/default.aspx?scid=kb;de;329170
- Q326830, *MS02-045: Ungeprüfter Puffer in Netzwerkfreigabe kann Dienstverweigerung verursachen* http://support.microsoft.com/default.aspx?scid=kb;de;326830
- IPSec kann computerbasierte Authentifizierung und Verschlüsselung für den gesamten Netzwerkverkehr zwischen zwei Computern gewährleisten, so dass die Daten unter voller

Kontrolle des Besitzers bleiben. Ein Datendiebstahl während der Übertragung kann zu katastrophalen Folgen für die Firma führen.

- IPSec muss in der Firewall eingerichtet werden, damit Pakete mit der IPSec-Protokollnummer durchgereicht werden. Dies sind ESP (Protokollnummer 50) und AH (Protokoll 51) Paket.
- IPSec benutzt den 3DES-Verschlüsselungsalgorithmus und den SHA1-Integritätsalgorithmus, und wurde nach den FIPS 140-1-Kriterien zertifiziert. Viele Regierungs- und Militärstellen, sowie Bereiche des Finanzsektors und der Gesundheitsorganisationen verlangen diese Zertifizierungen oder den FIPS 140-1 Standard, um damit den Netzwerkverkehr zu schützen. Der RC4 Stream-Verschlüsselungsalgorithmus wird standardmäßig dafür benutzt, Netzwerkverkehr der meisten Windowsprotokolle (RPC, Kerberos, und Lightweight Directory Access Protocol (LDAP) zu verschlüsseln. RC4 ist allerdings kein Teil einer Standardzertifizierung oder des FIPS 140-1 Zertifizierungsstandards.
- Als eine softwarebasierte Windows-Lösung ist IPSec kosteneffektiver beim Aufbau einer Rechner-zu-Rechner-Kommunikation als eine hardwarebasierte Lösung. Hardwarebasierte Sicherheitslösungen, wie die Unterhaltung eines virtuellen privaten Netzwerks (VPN) oder eine exklusiv gemietete Leitung, sind normalerweise teurer als die Windows-Lösung
- IPSec verbrauchen gegenüber dem Einsatz anderer protokollspezifischer Verschlüsselungen, wie zum Beispiel dem Signieren der SMB Kommunikation, weniger CPU-Zeit. Aktive IPSec-Netzwerkkarten können die von IPSec benutzten Verschlüsselungsoperationen beschleunigen. Als Ergebnis könnte es sein, dass IPSec verschlüsselte TCP/IP-Kommunikation denselben Durchsatz erreicht, wie unverschlüsselte TCP/IP-Kommunikation. Testen Sie auf jeden Fall vorher den jeweiligen Einfluss von Verschlüsselung auf Ihren Domänenkontrollern. Mehr Informationen zum Thema aktive IPSec-Netzwerkkarten und zu deren Vorteilen finden Sie im Internet unter *Intel PRO/100S Network Adapter, IPSec Offload Performance and Comparison* unter http://www.veritest.com/clients/reports/intel/intelps.pdf (englischsprachig).

Mögliche Auswirkungen

IPSec-Filter sind eine Möglichkeit den Server gegen Netzwerkangriffe zu schützen. Sie sollten nicht als Einzellösung betrachtet werden. IPSec wurde als Ersatz für existierende Firewall-Lösungen oder Routerfilter entwickelt. Es wird für einfache Paketfilterung empfohlen, um Clients und Server immer da zu sichern, wo statische Filterregeln effektiv verwendet werden können. Außerdem wurde IPSec so entwickelt, dass es durch Verzeichnisdienstrichtlinien auf viele Computer verteilt werden kann. Die folgenden Einschränkungen gelten für IPSec-Filter:

- IPSec-Filter können nicht für einzelne Anwendungen definiert werden. Es können lediglich Filterregeln für Protokolle und Ports eingerichtet werden.
- IPSec-Filter sind statisch.
- IPSec-Filter unterscheiden ICMP-Meldungen nicht.
- IPSec-Filter untersuchen keinen Inhalt von IP-Paketen um Einbruchserkennung (Intrusion Detection) zu betreiben.
- IPSec-Filter können sich überlappen, jedoch nicht von Hand sortiert werden. Der IPSec-Dienst berechnet die Gewichtung der Filter intern in Abhängigkeit von der IP-Adresse, dem Protokoll und dem Quell- und Zielport.
- IPSec sind nicht netzwerkschnittstellenspezifisch, dennoch können sie speziell für einzelne IP-Adressen gelten. Allerdings wird der gesamte Netzwerkverkehr auf einer Schnittstelle durch den Filter geschleust.
- IPSec-Filter können nicht explizit als eingehende oder ausgehende Filter eingestellt werden. Eingehend oder ausgehend Richtung wird in Abhängigkeit der im Filter verwendeten IP-Adressen bestimmt. In einigen Fällen werden beide - eingehende wie ausgehende Filter automatisch generiert.
- IPSec unterstützt keine doppelten Filter.

- Obwohl Windows Server 2003 eine deutlich bessere IPSec-Filterleistung bietet, kann die CPU-Leistung bei viel Netzwerkverkehr nachlassen.

Sollte ein IPSec-Filter (oder ein anderes Netzwerkgerät) bestimmten Netzwerkverkehr abblocken, kann dies zu ungewöhnlichem Anwendungsverhalten und Ereignisanzeigen führen. IPSec-Filter erzeugen bei verworfenen Paketen schwer zu lesende Protokolleinträge. Der Netzwerkmonitor (Netmon) kann keine ausgehenden, abgeblockten Pakete mitschneiden oder darstellen. Eingehende Pakete können durch den Netzwerkmonitor mitgeschnitten werden, allerdings wird sich in den mitgeschnittenen Paketen kein Eintrag finden, dass diese Pakete verworfen wurden.

Weiterhin sollte ein durchdachtes Design der Filterregeln für Anwendungen auf einer vorherigen detaillierten Analyse des Netzwerkes und der Ereignisse beruhen. Beispielsweise benutzt das SMB-Protokoll den TCP Port 139 für Dateitransfer, Datei- und Druckfreigaben. Sollten Sie diesen Port durch IPSec-Filter abblocken, kann SMB immer noch den TCP Port 445 benutzen. Ein anderes Beispiel ist eine Situation, bei der eine Anwendung mehrere Protokolle mit mehreren Zieladressen verwendet. SMB und andere Protokolle benutzen normalerweise auch eine Form der Benutzerauthentifizierung. Diese führt dazu, dass ein Domänencontroller gefunden werden muss, und danach mit dem Kerberosprotokoll die eigentliche Authentifizierung stattfindet. Kerberos benutzt zum suchen der Domänenkontroller eine DNS-Abfrage auf UDP oder TCP Port 53. Nachdem die IP-Adresse des Domänencontrollers bekannt ist, kann eine LDAP-Anfrage auf Port UDP 389 gestellt werden. Danach kann über UDP oder TCP Port 88 eine Authentifizierung durchgeführt werden. Andere Protokolle, wie zum Beispiel RPC, benutzen einen breiten TCP Port Bereich. Dieser wird bei Start des Computers dynamisch bestimmt. Somit können RPC basierte Anwendungen mit einem statischen Portfilter nicht kontrolliert werden, außer es besteht die Möglichkeit die Anwendung so zu konfigurieren, dass nur bestimmte Ports verwendet werden.

Unter Windows 2000 und Windows XP werden Standardausnahmen in den IPSec-Richtlinien eingesetzt, damit IP-Verkehr der nicht durch IKE gesichert werden kann nutzbar ist. Dies sind beispielsweise Pakete, die den Quality of Service (QoS) für IPSec-Verkehr mit dem RSVP (Resource Reservation Protokoll) Protokoll benutzen, oder aber IPSec-Funktionalitäten, die Teil des IPSec-Mechanismus sind. Ein Registrierungsschlüssel, der diese Ausnahmen wieder entfernt, wurde von Microsoft veröffentlicht. Mehr Informationen zu diesem Thema finden Sie in dem Microsoft Knowledge Base-Artikel Q811832 *IPSec Default Exemptions Can Be Used to Bypass IPSec Protection in Some Scenarios*, unter dem Link: http://support.microsoft.com/default.aspx?scid=811832 (englischsprachig) und dem Microsoft Knowledge Base-Artikel Q810207, *IPSec Default Exemptions Are Removed in Windows Server 2003,* unter http://support.microsoft.com/default.aspx?scid=810207 (englischsprachig).

Wird ein Windows 2000-Computer mit dem Internet verbunden, erlaubt der gespiegelte ausgehende Filter (wie oben für Port 80) einem Angreifer Zugang zu jedem offenen TCP Port auf Ihren Server. Somit kann ein Fehler in der IPSec-Konfiguration zum Verlust der erwarteten Sicherheit führen. Testen Sie daher immer Ihre Konfiguration, damit die erwartete Sicherheit gegen Angriffe auch ordnungsgemäß vorhanden ist. Ein Sicherheitsloch, welches dazu führt, dass ein Angreifer lokaler Administrator wird oder mit dem lokalen Systemkonto arbeiten kann, erlaubt dem Angreifer auch die IPSec-Sicherheitsrichtlinien zu ändern oder abzuschalten.

IPSec in Windows 2000 bietet keine komplette Filterung während des Hochfahrens. Es gibt dabei ein kleines Zeitfenster, in dem der TCP/IP Protokollstapel schon reagiert ohne zu filtern. Ein automatischer Angriff kann zu diesem Zeitpunkt auf Anwendungsports zugreifen, die später dann durch IPSec abgeblockt werden. In den meisten Fällen sind die Anwendungen allerdings nicht in der Lage Verbindungen aufzubauen, bevor IPSec die Filterung übernimmt. Um den höchsten Grad an IPSec-Sicherheit zu erreichen, trennen Sie den Computer während eines Neustarts vom Netzwerk. Windows Server 2003 bietet eine extra Richtlinie für das Hochfahren des Systems.

Weder Windows 2000 noch Windows Server 2003 wurden mit der Möglichkeit ausgestattet, Abhängigkeiten der Dienste des IPSec-Richtlinienagenten beim Dienststart zu definieren. Die wird nicht garantiert, dass die Filter schon arbeiten, bevor der Dienst startet.

Der Windows Server 2003 bietet die Internet Connection Firewall (ICF). ICF kann ein lesbares Protokoll für abgeblockte eingehende und ausgehende Pakete erstellen. Allerdings dient ICF nicht dazu, eine zentrale Verwaltung von Regeln vorzunehmen oder Pakete nach Quelladressen zu filtern.

ICF kann in Kombination mit IPSec-Filtern benutzt werden. Dabei könnte in den Fällen, in denen IPSec mit einem gespiegelten Filter eingerichtet wurde, der Schutz vor Angriffen durch ICF-Routinen gesichert werden. Allerdings sollten Router oder Firewallsysteme immer als erste Filtermechanismen gegen Angriffe benutzt werden.

Ein rechnerbasiertes Intrusion Detection System oder ein anderes Antivirensystem sind ebenfalls empfehlenswert, damit Einbrüchen oder Infektionen effektiv entgegengewirkt werden kann.

Obwohl der IPSec die Sicherheit deutlich verbessern kann, sollten Sie bedenken, dass beim seinem Einsatz zusätzlich Ausbildungs- und Administrationskosten und höhere Hardwarekosten, zum Beispiel wenn Sie IPSec-Hardware, aktive IPSec-Netzwerkkarten oder mehr CPU Kapazität einsetzen, entstehen.

Die Einrichtung von IPSec mit AH fordert einen zusätzlichen Aufwand für Client/ Serverumgebungen. Die IPSec-Konfiguration und die Vertrauensstellungen zwischen Client und Servern müssen entsprechend eingerichtet werden. Sollten sich zwei Computer immer in der gleichen Domäne oder in sich vertrauendenden Domänen befinden, kann eine Grupperichtlinie die erforderliche Sicherheit mittels IPSec und Kerberos-Authentifizierung einrichten. Kerberos ist in diesem Falle auch für die Vertrauensstellung verantwortlich. Kann ein Computer das Kerberos-Protokoll nicht benutzen, müssen entweder Computerzertifikate oder gemeinsame Schlüssel verwendet werden. Dieses Handbuch empfiehlt allerdings keine Verwendung gemeinsamer Schlüssel, da deren Wert ungesichert in der IPSec-Richtlinie gespeichert wird. Die im Active Directory gespeicherte Richtlinie sollte jedoch für alle Domänencomputer zugänglich sein. Aus diesem Grund ist es schwer, den gemeinsamen Schlüssel geheim zu halten. Microsoft empfiehlt digitale Zertifikate, falls der Einsatz von Kerberos für die IKE-Authentifizierung nicht möglich sein sollte.

Weitere Informationen über die Windows IPSec-Implementierung finden Sie im Internet auf der Windows 2000 IPSec-Webseite unter http://www.microsoft.com/windows2000/technologies/communications/ipsec/default.asp (englischsprachig).

12

Zusammenfassung

In diesem Handbuch wurden die wichtigsten Sicherheitsmaßnahmen erklärt, die Ihnen unter Microsoft® Windows Server 2003 und Microsoft Windows® XP Professional zur Verfügung stehen. Die meisten der empfohlenen Einstellungen können über Sicherheitsvorlagen und Gruppenrichtlinienobjekte (GPOs) umgesetzt werden. Andere werden über den Bereich administrative Vorlagen (ADM) der Gruppenrichtlinien umgesetzt. Einige Absicherungsverfahren können jedoch auf diesem Weg nicht durchgeführt werden. Das Handbuch beschreibt, wie diese Verfahren manuell umgesetzt werden.

Weitere Informationen

Weitere Informationen zur Sicherheit und zum Datenschutz bei Microsoft finden Sie unter http://www.microsoft.com/germany/ms/security/

Weitere Informationen zu Sicherheitsbedrohungen und zu Verfahren, um diese zu minimieren, finden Sie unter http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/secthret.asp (englischsprachig).

Weitere Informationen zu den "Zehn unveränderlichen Gesetzten der Sicherheit“ finden Sie unter http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/10imlaws.asp (englischsprachig).

Weitere Informationen zur Sicherheit unter Windows Server 2003 finden Sie unter http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_SEtopnode.asp (englischsprachig).

Weitere Informationen zu Designüberlegungen zur Delegierung der Administration von Microsoft Active Directory® finden Sie unter http://www.microsoft.com/technet/prodtechnol/ad/windows2000/plan/addeladm.asp (englischsprachig).

Weitere Informationen zu den unterschiedlichen Arten von Netzwerkangriffen finden Sie im Dokument "Common Types of Network Attacks", dass dem Windows 2000 Server Resource Kit entnommen wurde, unter http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/cnet/cndb_ips_ddui.asp (englischsprachig).

Weitere Informationen zur Absicherung des Windows Server 2003 TCP/IP-Protokollstacks finden Sie im Knowledge Base Artikel Q324270 *Harden the TCP/IP Stack Against Denial of Service Attacks in Windows Server 2003* unter http://support.microsoft.com/default.aspx?scid=324270 (englischsprachig).

Weitere Informationen zur Absicherung von Windows Socket-Anwendungen finden Sie im Knowledge Base Artikel Q142641 *Internet Server Unavailable Because of Malicious SYN Attacks* unter http://support.microsoft.com/default.aspx?scid=142641 (englischsprachig).

Weitere Informationen zu .adm-Dateien finden Sie im Knowledge Base Artikel Q228460 *Location of ADM (Administrative Template) Files in Windows* unter http://support.microsoft.com/default.aspx?scid=228460 (englischsprachig).

Weitere Informationen zur Anpassung des Sicherheitskonfigurationseditors finden Sie im Microsoft Knowledge Base Artikel Q214752 *How to Add Custom Registry Settings to Security Configuration*

Editor unter
http://support.microsoft.com/default.aspx?scid=214752 (englischsprachig).

Weitere Informationen zur Erstellung von angepassten administrativen Vorlagen finden Sie im Microsoft Knowledge Base Artikel Q323639 *How to: Create Custom Administrative Templates in Windows 2000* unter
http://support.microsoft.com/default.aspx?scid=323639 (englischsprachig).

Lesen Sie außerdem das Whitepaper *Implementing Registry-Based Group Policy* unter
http://www.microsoft.com/WINDOWS2000/techinfo/howitworks/management/rbppaper.asp
(englischsprachig).

Weitere Informationen zur Verwendung der LAN-Manager-Authentifizierung in Netzwerken mit Windows 2000- und Windows NT® 4.0-Systemen finden Sie im Microsoft Knowledge Base Artikel Q305379 *Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain* unter
http://support.microsoft.com/default.aspx?scid=Q305379 (englischsprachig).

Weitere Informationen zur LAN-Manager-Kompatibilität finden Sie unter
http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/regentry/76052.asp (englischsprachig).

Weitere Informationen zur NTLMv2-Authentifizierung finden Sie im Microsoft Knowledge Base Artikel Q239869 *How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT* unter
http://support.microsoft.com/default.aspx?scid=239869 (englischsprachig).

Weitere Informationen zu den Standardeinstellungen der Dienste unter Windows Server 2003 finden Sie unter
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/datacenter/sys_srv_default_settings.asp (englischsprachig).

Weitere Informationen zur Bereitstellung von Smarcards finden Sie auf der TechNet Smart Card-Webseite unter
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/smrtcard/default.asp (englischsprachig).

Weitere Informationen zu Überwachungsrichtlinie unter Windows Server 2003 finden Sie unter
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/APtopnode.asp (englischsprachig).

Weitere Informationen zur Zuweisung von Benutzerrechten unter Windows Server 2003 finden Sie unter
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/URAtopnode.asp (englischsprachig).

Weitere Informationen zur Absicheurng des Terminaldienstes finden Sie im Dokument *Securing Windows 2000 Terminal Services* (Die Informationen in diesem Artikel gelten auch für Windows Server 2003) unter
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/win2kts/maintain/optimize/secw2kts.asp (englischsprachig).

Weitere Informationen zur Wiederherstellung der Standardwerte der Sicherheitseinstellungen finden Sie im Microsoft Knowledge Base Artikel Q313222 *How to: Reset Security Settings Back to the Defaults* unter
http://support.microsoft.com/default.aspx?scid=313222 (englischsprachig).

Weitere Informationen zur Wiederherstellung der Standardwerte der Sicherheitseinstellungen in der Default Domain Policy finden Sie im Microsoft Knowledge Base Artikel Q324800 *Reset User Rights in the Default Domain Group Policy in Windows Server 2003* unter
http://support.microsoft.com/default.aspx?scid=324800 (englischsprachig).

Weitere Informationen zur Sicherheit unter den verschiedenen Windows-Betriebssystemen finden Sie im *Microsoft Windows Security Resource Kit*. Informationen darüber, wie Sie dieses Buch erwerben können finden Sie unter
http://www.microsoft.com/MSPress/books/6418.asp (englischsprachig).

Weitere Informationen zum *Office XP Resource Kit* oder zum Herunterladen des *Office Resource Kit Tools* finden Sie unter
http://www.microsoft.com/office/ork/xp/default.htm und
http://www.microsoft.com/office/ork/xp/appndx/appc00.htm (englischsprachig).