3 Verarbeitungsreihenfolge von Gruppenrichtlinien

Dieses Kapitel behandelt folgende Themen:

- In welcher Reihenfolge werden Gruppenrichtlinienobjekte verarbeitet?
- Wie wird die Verarbeitungsreihenfolge durch Erzwungen und Vererbung deaktivieren beeinflusst?
- Was ist der Loopback-Verarbeitungsmodus?
- Gruppenrichtlinienobjekte teilweise oder ganz deaktivieren

3.1 Einführung

Was passiert eigentlich genau, wenn eine Gruppenrichtlinie angewendet wird? Es werden Registrierungs-Schlüssel angewendet. Aber warum, in welcher Reihenfolge und welche Auswirkungen hat dies auf das System?

Ein tieferes Verständnis der Reihenfolge, in der Gruppenrichtlinien angewendet werden, ist ausschlaggebend für deren korrekten und effizienten Einsatz. Durch geschickten Umgang mit der Platzierung von Richtlinien lässt sich deren Anzahl minimieren und Änderungen können bei Bedarf schnell und effektiv eingepflegt werden. Darüber hinaus gibt es Methoden, mit denen Sie die Verarbeitungsreihenfolge beeinflussen können.

In diesem Kapitel erfahren Sie, wie Sie die Verarbeitung der GPOs über die Group Policy Management Console (GPMC) verwalten können. Einen tieferen Einblick in die Vorgänge, die während der Gruppenrichtlinienverarbeitung ablaufen, erhalten Sie in Kapitel 12, Funktionsweise von Gruppenrichtlinien.

3.2 Grundlagen der Gruppenrichtlinienverarbeitung

Gruppenrichtlinien werden von Windows seit Vista mithilfe eines eigenständigen Dienstes, des Gruppenrichtliniendiensts, verarbeitet. Der Gruppenrichtliniendienst ist dafür verantwortlich, die GPOs aus der Domäne zu verarbeiten und Computer- bzw. Benutzereinstellungen anzuwenden.

Der Gruppenrichtlinienclient startet die Gruppenrichtlinienverarbeitung automatisch beim Systemstart, bei jeder Benutzeranmeldung und zeitgesteuert alle 90 bis 120 Minuten. Die Verarbeitung erfolgt dabei für Computer und Benutzer unabhängig.

Der Gruppenrichtlinienclient verarbeitet nur Einstellungen, die auch tatsächlich konfiguriert sind. Das klingt trivial, ist es aber nicht. Denn Sie haben speziell in den administrativen Vorlagen der GPOs immer die Möglichkeit, eine Einstellung auf „Aktiviert“, „Deaktiviert“ oder „Nicht konfiguriert“ zu setzen. Nicht konfiguriert bedeutet, dass die Gruppenrichtlinie nicht angepasst wird, also weder ein- noch ausgeschaltet ist. Deaktiviert dagegen bedeutet, dass eine Einstellung explizit ausgeschaltet wird.

3.3 Verarbeitungsreihenfolge in der Gruppenrichtlinienverarbeitung

Eine GPO besteht immer aus zwei Einstellungsknoten – einer Computerkonfiguration und einer Benutzerkonfiguration. Eigentlich haben wir es hier nicht mit einer, sondern mit zwei GPOs zu tun, da die Computereinstellungen und die Benutzereinstellungen nicht gleichzeitig vorgenommen werden!

Wenn ein Computer gestartet wird, dann fängt der Gruppenrichtlinienclient an, den Computer anhand der Computerrichtlinien zu konfigurieren. Hierfür schaut er nach, in welcher Organisationseinheit sich das Computerkonto befindet, listet die Gruppenrichtlinien auf, die für den Computer gültig werden, und liest danach die Einstellungen vom Domänen-Controller. Hierfür verarbeitet er nur die Einstellungen aus den Computerkonfigurationen – logisch, es handelt sich ja um einen Computer.

Wenn sich jetzt ein Benutzer am Computer anmeldet, dann startet der Gruppenrichtliniendienst das gleiche Prozedere. Er schaut nach, wo sich der Benutzer im AD befindet, listet alle Gruppenrichtlinien auf, die für den Benutzer gelten, liest die Einstellungen (dieses Mal die Benutzerkonfiguration) vom Domänencontroller und wendet die Einstellungen auf den Benutzer an. Wenn sich der Benutzer und der PC nicht in der gleichen OU befinden, bedeutet dies aber, dass für den Benutzer und den Computer völlig unterschiedliche Gruppenrichtlinien gezogen wurden! Es gibt also faktisch eigentlich in jeder Gruppenrichtlinie immer zwei Gruppenrichtlinien – eine für Computer (Computerkonfiguration) und eine für Benutzer (Benutzerkonfiguration). Diese haben miteinander nichts zu tun!

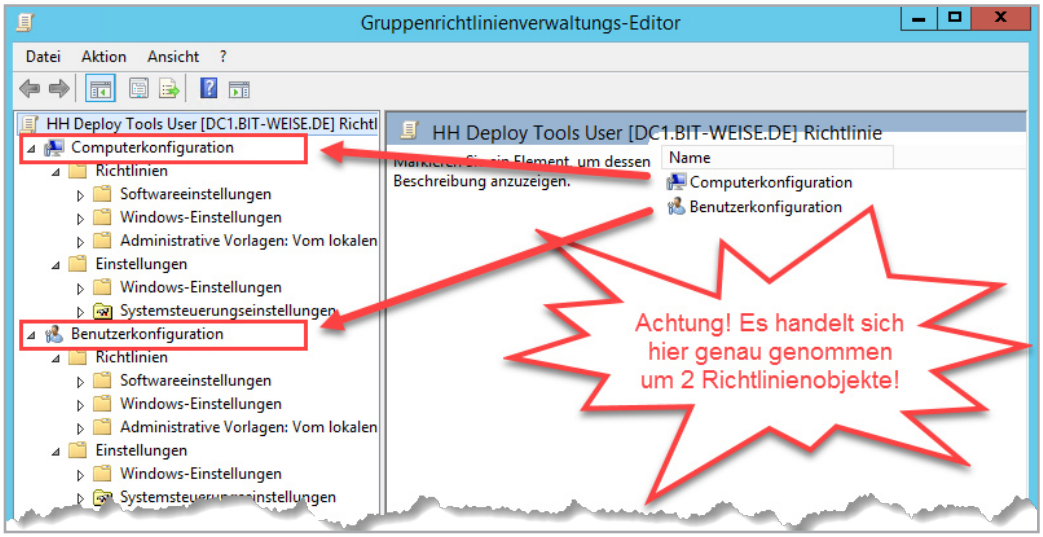

Bild 3.1 Computer- und Benutzerkonfiguration werden getrennt verarbeitet.

Ein kleines Beispiel zur Verdeutlichung:

Der Benutzer Hans befindet sich in der Organisationseinheit IT in Hamburg. Für einen Besuch in Hannover meldet er sich am PC seines Kollegen an. Der PC befindet sich in der OU Computer in Hannover. Wenn der Benutzer Hans sich am Laptop anmeldet, wertet der Gruppenrichtlinienclient aus, in welcher OU sich das Benutzerkonto befindet, und wendet dann (in dieser Reihenfolge) die Gruppenrichtlinien

1. Default Domain Policy
2. HH Deploy Tools User
3. HH Config Base User

an.

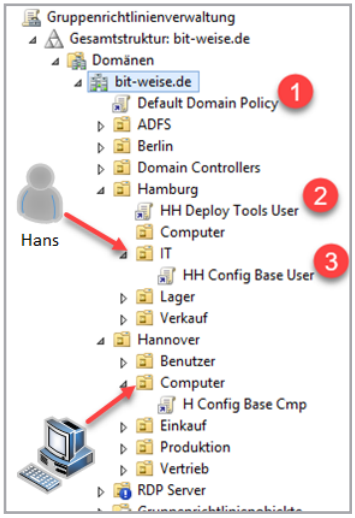

Bild 3.2
Der Benutzer kommt aus Hamburg, der Computer aus Hannover.

Wenn sich in der Richtlinie „H Config Base Cmp“ die Einstellung aus der unten stehenden Abbildung befindet, wirkt sich diese Einstellung auf den Benutzer aus?

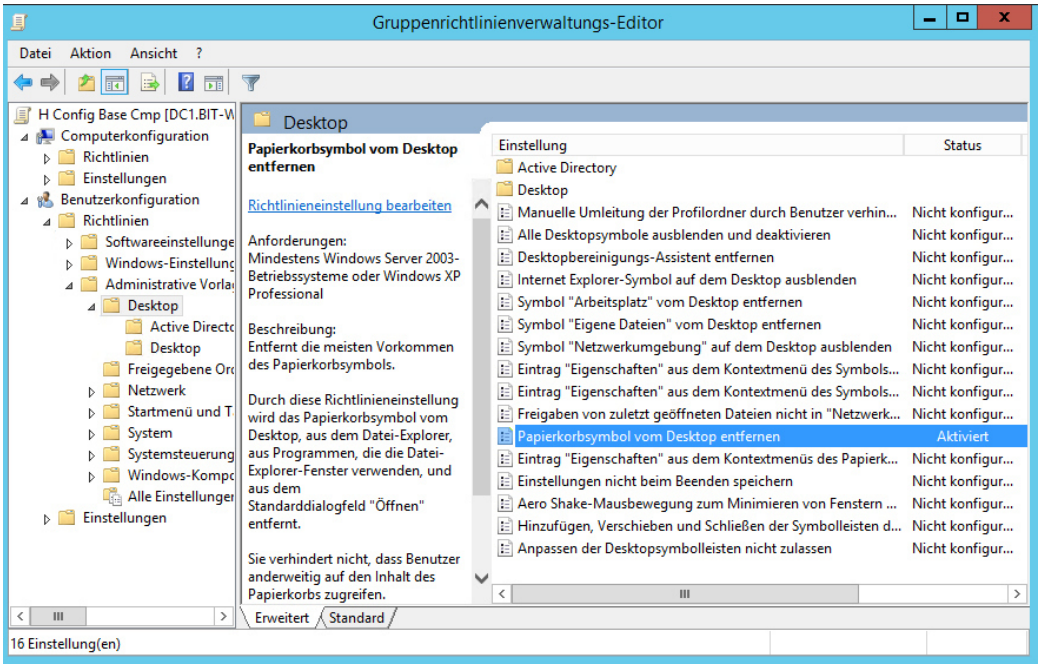

Bild 3.3 In dem GPO wird der Papierkorb für Benutzer vom Desktop ausgeblendet.

Die Antwort lautet nein, da sie zwar in der Benutzerkonfiguration gesetzt ist, aber in der des Computers, und die wird für den Benutzer gar nicht angewendet!

3.4 Anpassungen der Verarbeitungsreihenfolge von GPOs

Sie können die Verarbeitungsreihenfolge von GPOs beeinflussen. So können etwa Einstellungen erzwungen und die Vererbung von übergeordneten Richtlinien abgelehnt werden, die Bereiche Computerkonfiguration oder Benutzerkonfiguration lassen sich deaktivieren, und die Übernahme von Richtlinien kann durch Gruppenzugehörigkeiten gefiltert werden. Im Folgenden werden die einzelnen Funktionen kurz erläutert.

3.4.1 Bereiche von GPOs deaktivieren

Sie können in einer GPO festlegen, dass nur ein Teilbereich aktiviert werden soll. Dies kann entweder der Teilbereich Benutzerkonfiguration sein, der Teilbereich Computerkonfiguration oder beide Bereiche. Dann ist die gesamte Gruppenrichtlinie außer Funktion. Dies kann etwa sinnvoll sein, wenn eine GPO deaktiviert, aber nicht gelöscht werden soll.

HINWEIS: Der Objektstatus einer Gruppenrichtlinie ist nicht auf eine Verknüpfung beschränkt. Wenn ein Teilbereich deaktiviert ist, wirkt sich das auf alle Verknüpfungen der GPO aus!

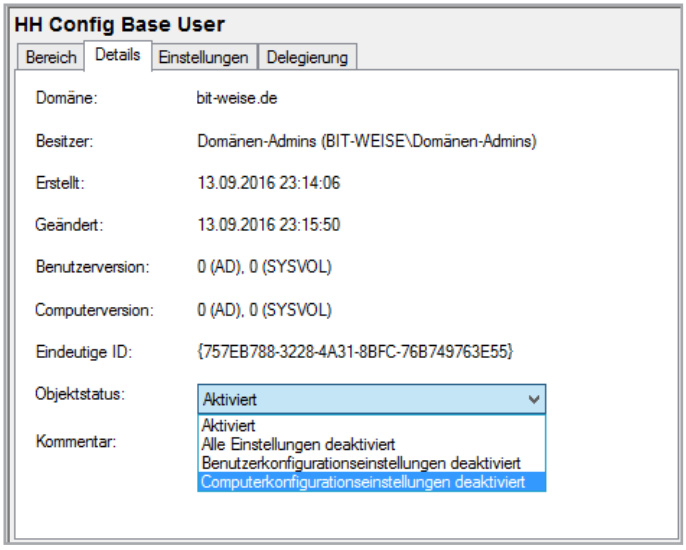

Bild 3.4 Bereiche einer GPO deaktivieren

Um Bereiche einer Gruppenrichtlinie zu deaktivieren gehen Sie folgendermaßen vor:

Navigieren Sie in der Gruppenrichtlinienverwaltungskonsole auf die Gruppenrichtlinienverknüpfung oder das Gruppenrichtlinienobjekt, das Sie bearbeiten möchten, und wählen Sie im rechten Fenster das Register DETAILS. Dann können Sie im Rollfeld OBJEKTSTATUS die entsprechende Einstellung auswählen.

Um zu überprüfen, welche Gruppenrichtlinien in welchen Bereichen aktiv sind, können Sie in der Gruppenrichtlinienverwaltungskonsole auf die Organisationseinheit navigieren, mit der die GPOs verknüpft sind. Im rechten Fenster können Sie dann die Spalte OBJEKTSTATUS überprüfen.

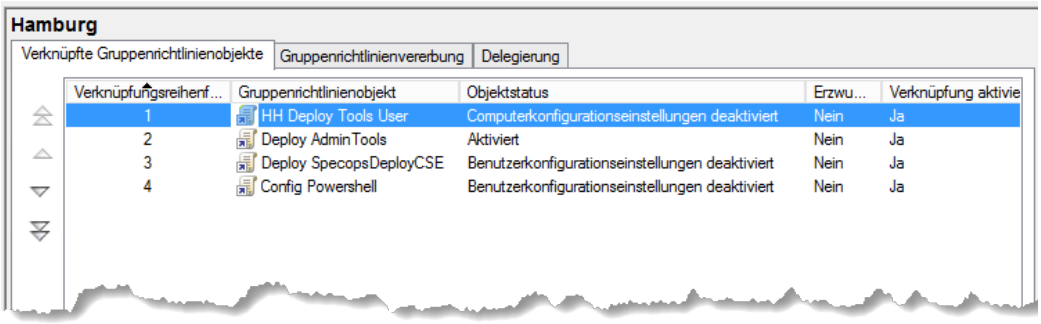

Bild 3.5 Objektstatus von GPOs prüfen

3.4.2 Verknüpfungen aktivieren/deaktivieren

Sie können auch eine einzelne Verknüpfung einer Gruppenrichtlinie mit einer Organisationseinheit deaktivieren oder aktivieren. Dies gilt aber stets für alle Bereiche der GPO.

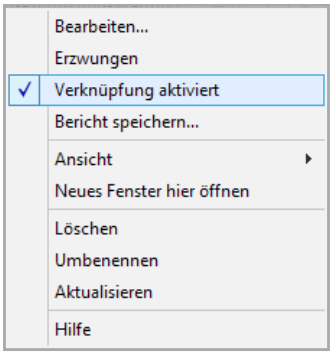

Bild 3.6
Verknüpfungseigenschaften bearbeiten

Öffnen Sie das Kontextmenü einer Gruppenrichtlinienverknüpfung, um diese zu deaktivieren oder zu aktivieren.

Den Status einer Gruppenrichtlinienverknüpfung können Sie überprüfen, indem Sie die zugehörige Organisationseinheit in der Gruppenrichtlinienverwaltungskonsole aufrufen. Deaktivierte Verknüpfungen sind heller dargestellt und im rechten Fenster ist der Verknüpfungsstatus mit Ja/Nein gekennzeichnet.

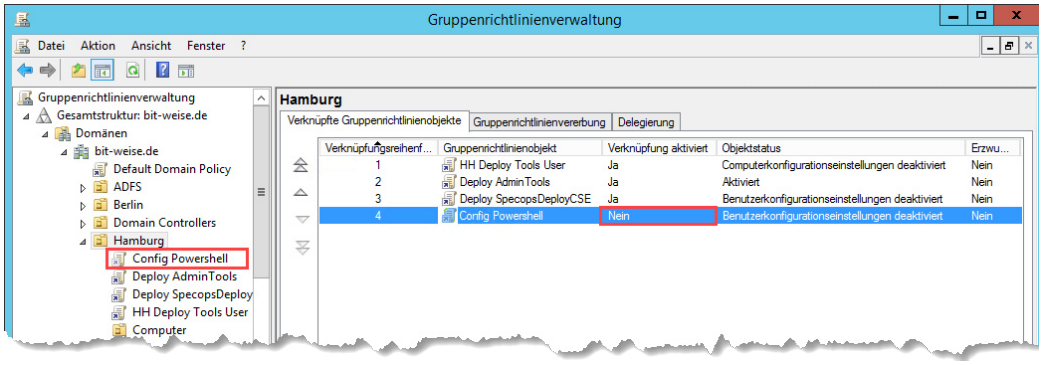

Bild 3.7 Verknüpfungsstatus überprüfen

3.4.3 Vererbung deaktivieren

Sie können für eine Organisationseinheit festlegen, dass diese keine übergeordneten Richtlinien übernehmen soll. Dies bezeichnet man als VERERBUNG DEAKTIVIEREN, obwohl die Vererbung eigentlich gar nicht deaktiviert, sondern nur die Vererbung von übergeordneten GPOs blockiert wird. Untergeordnete Organisationseinheiten erben auch weiterhin die Gruppenrichtlinien einer Organisationseinheit mit deaktivierter Vererbung!

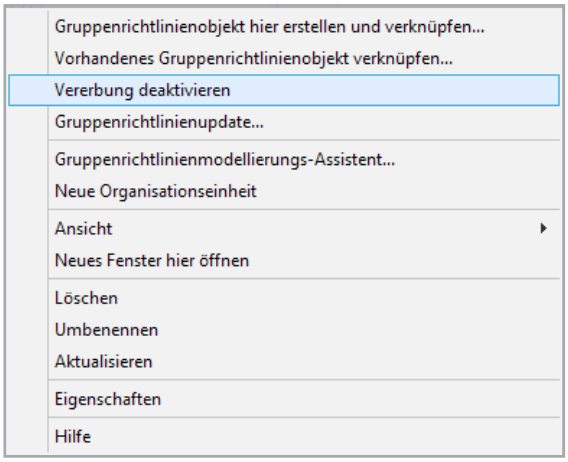

Bild 3.8 Vererbung deaktivieren

Um die Vererbung von Gruppenrichtlinien für eine Organisationseinheit zu deaktivieren, navigieren Sie in der Konsolenstruktur auf die Organisationseinheit, öffnen Sie das Kontextmenü und klicken Sie auf VERERBUNG DEAKTIVIEREN. Die Organisationseinheit ist nun mit einem Ausrufezeichen in einem blauen Kreis gekennzeichnet.

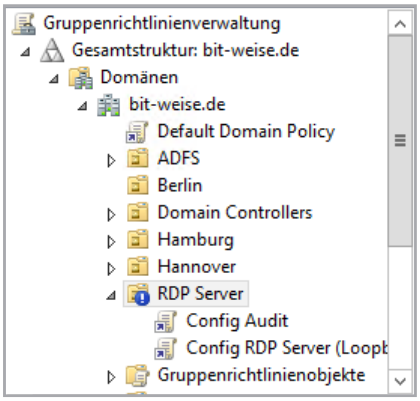

Bild 3.9
Organisationseinheit mit deaktivierter Vererbung

3.4.4 Erzwingen von GPOs

Wenn Sie sicherstellen möchten, dass die Einstellungen einer GPO nicht überschrieben werden, können Sie diese mit einem Schreibschutz versehen. Klicken Sie hierzu mit der rechten Maustaste auf die Gruppenrichtlinienverknüpfung und aktivieren Sie im Kontextmenü den Befehl Erzwungen.

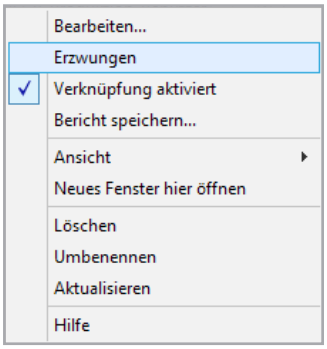

Bild 3.10
Kontextmenübefehl Erzwungen

Erzwungene GPOs lassen sich durch nachfolgende GPOs nicht mehr überschreiben. Dies ist in der Konsolenstruktur durch ein Vorhängeschloss auf der Gruppenrichtlinienverknüpfung markiert. Außerdem durchbricht eine erzwungene Richtlinie die Vererbungsblockierung – sie wird also immer gültig.

Achten Sie darauf, dass eine erzwungene GPO schreibgeschützt ist und von einer tiefer liegenden, ebenfalls erzwungenen GPO nicht überschrieben werden kann. Erzwingen dreht effektiv also die Priorität der GPOs um.

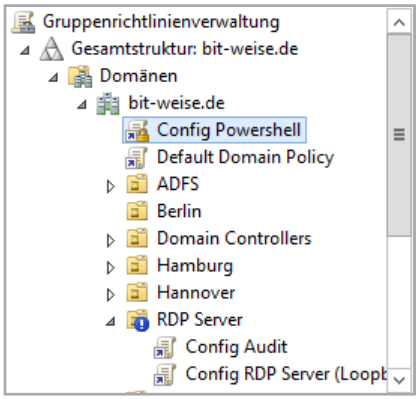

Bild 3.11
Erzwungene Gruppenrichtlinienverknüpfung

HINWEIS: Das Erzwingen sollten Sie meiden wie der Teufel das Weihwasser, auch wenn es Ihnen im Notfall gerade sinnvoll erscheint, mal schnell die Einstellung zu erzwingen, die aus unerfindlichen Gründen nicht angewendet wird im AD – Sie vergessen hinterher (ich wette um eine Kiste Bier), die Einstellung wieder rückgängig zu machen, und beim nächsten Mal müssen Sie eine weitere GPO erzwingen, weil Ihre Verarbeitung einfach nicht funktionieren will …

Der Sinn von Erzwingen ist es, Sicherheitseinstellungen, die z. B. aufgrund von Sicherheitsrichtlinien immer auf allen Computer gesetzt sein müssen, gegen alle Widerstände durchzusetzen. Nur hierfür sollte diese Option auch eingesetzt werden.

3.4.5 Gruppenrichtlinien filtern

Standardmäßig werden Gruppenrichtlinien bei der Erstellung mit der Berechtigung Gruppenrichtlinie übernehmen für die Gruppe „Authentifizierte Benutzer“ angelegt.

Wenn Sie nur bestimmten Gruppen von Benutzern oder Computern das Übernehmen von Gruppenrichtlinieneinstellungen erlauben wollen, können Sie die Gruppenrichtlinie filtern:

- Sie können positive Filter verwenden, wenn nur die Mitglieder einer ausgewählten Gruppe die Einstellungen übernehmen sollen.
- Mit negativen Filtern verweigern Sie den Mitgliedern einer ausgewählten Gruppe die Anwendung der GPO.

3.4.5.1 Positive Sicherheitsfilterung

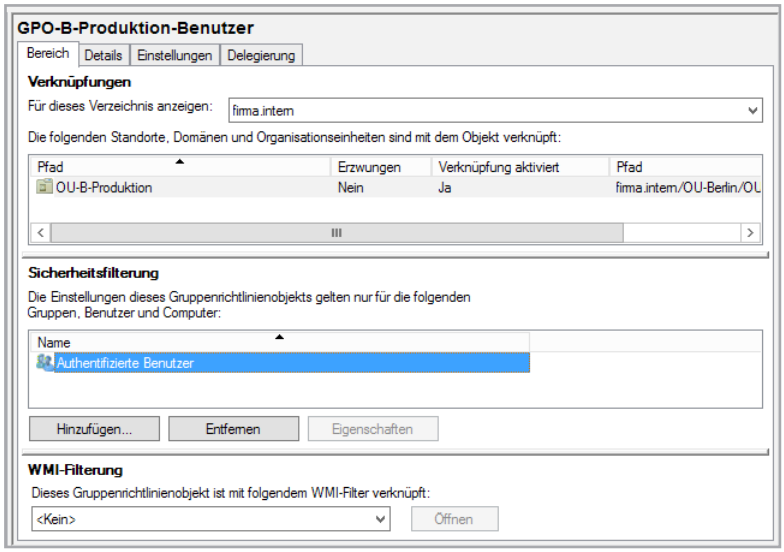

Bild 3.12 Sicherheitsfilterung einer Gruppenrichtlinie

Die positive Sicherheitsfilterung können Sie anpassen, indem Sie im Register Bereich einer Gruppenrichtlinie unter Sicherheitsfilterung auf die Schaltfläche Hinzufügen klicken und dann wie gewohnt eine Gruppe auswählen. Dies ergibt jedoch nur einen Sinn, wenn Sie die Gruppe „Authentifizierte Benutzer“ entfernen, da alle Benutzer (und Computer) zu den Authentifizierten Benutzern gehören.

ACHTUNG! Am 15. Juni 2016 hat Microsoft das Sicherheits-Patch MS16-072 verteilt, das eine Man-in-the-Middle Attack verhindern soll und bei einigen Firmen zu großem Chaos geführt hat, die mit Sicherheitsfilterung arbeiten. Das Patch MS16-072 soll verhindern, dass ein Angreifer Ihren Clients falsche GPOs unterjubelt. Dafür hat Microsoft das Verhalten des Gruppenrichtlinienclients so umgestellt, dass er sich jetzt mit dem Computerkonto am Domänencontroller anmeldet und nicht mehr wie bisher mit dem Benutzerkonto des Benutzers, der gerade verarbeitet wird. Haben Sie die Gruppe authentifizierte Benutzer aus der Sicherheitsfilterung entfernt und dem Computerkonto keine Berechtigungen gegeben, kann der Gruppenrichtlinienclient die GPOs nicht mehr vom Server abrufen und anwenden! Um dieses Problem zu lösen, müssen Sie den Computerkonten zumindest Lese-Rechte auf die GPOs geben. Dies geschieht über das Register Delegierung – siehe den folgenden Abschnitt „Negative Sicherheitsfilterung“.

Mehr Infos finden Sie unter *https://support.microsoft.com/en-us/kb/3163622* und beim GPO-Guy: *https://sdmsoftware.com/group-policy-blog/bugs/new-group-policy-patch-ms16-072-breaks-gp-processing-behavior/*

3.4.5.2 Negative Sicherheitsfilterung

Die negative Sicherheitsfilterung stellt eine komplexere Aufgabe dar. Um sie auszuführen, müssen in den erweiterten Sicherheitsberechtigungen der Gruppe explizite Einstellungen vorgenommen werden. Verfahren Sie dazu wie folgt.

Öffnen Sie das Register DELEGIERUNG der Gruppenrichtlinie und klicken Sie auf die Schaltfläche ERWEITERT.

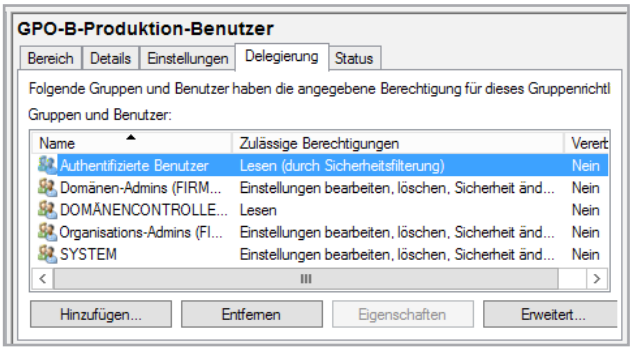

Bild 3.13 Einrichten negativer Sicherheitsfilterung

Wählen Sie nun die Gruppe aus, für die Sie die Sicherheitsfilterung einrichten möchten, und markieren Sie bei „Gruppenrichtlinie übernehmen“ das Kontrollkästchen für VERWEIGERN. Bestätigen Sie Ihre Konfiguration mit ÜBERNEHMEN.

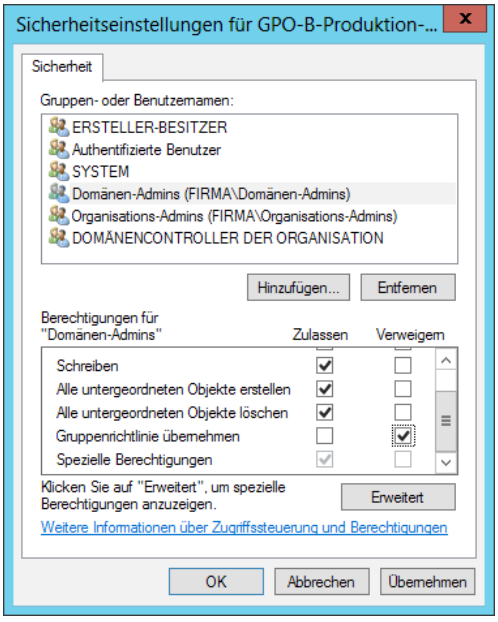

Bild 3.14
Übernehmen verweigern

Sie erhalten nun eine Warnmeldung, die besagt, dass Zugriffsverweigerungen stets Vorrang haben. Setzen Sie den Vorgang mit JA fort.

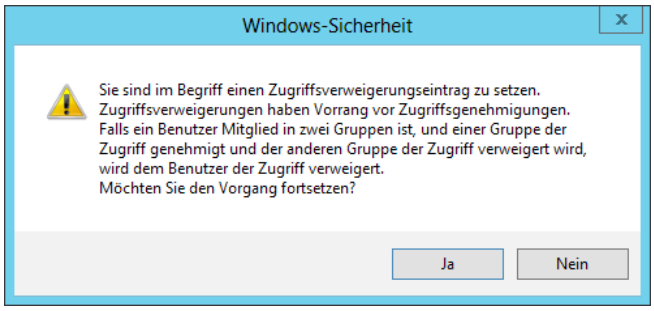

Bild 3.15
Warnung vor Zugriffsverweigerung

Wenn Sie mit der Sicherheitsfilterung arbeiten, können Sie hier auch der Gruppe „Domänencomputer“ die Berechtigung Lesen vergeben, um die Probleme von Fix MS16-072 zu beheben.

3.5 Praktisches Beispiel für die Verarbeitungsreihenfolge von Gruppenrichtlinien

Das folgende Beispiel verdeutlicht, wie in der Praxis mit Gruppenrichtlinien gearbeitet wird und welche Rolle dabei die Reihenfolge der Richtlinienverarbeitung spielt. Sie administrieren das Netzwerk eines mittelständischen Unternehmens in der Metallverarbeitung. Das Unternehmen hat zwei Standorte, die Hauptniederlassung in Berlin und eine Außenstelle in München. An beiden Standorten sind Produktionsabteilungen, in denen unter anderem CAD-Systeme eingesetzt werden. Mobile Mitarbeiter setzen tragbare Rechner an beiden Standorten ein.

Betrachten Sie zur Verdeutlichung die OU-Struktur in Bild 3.16.

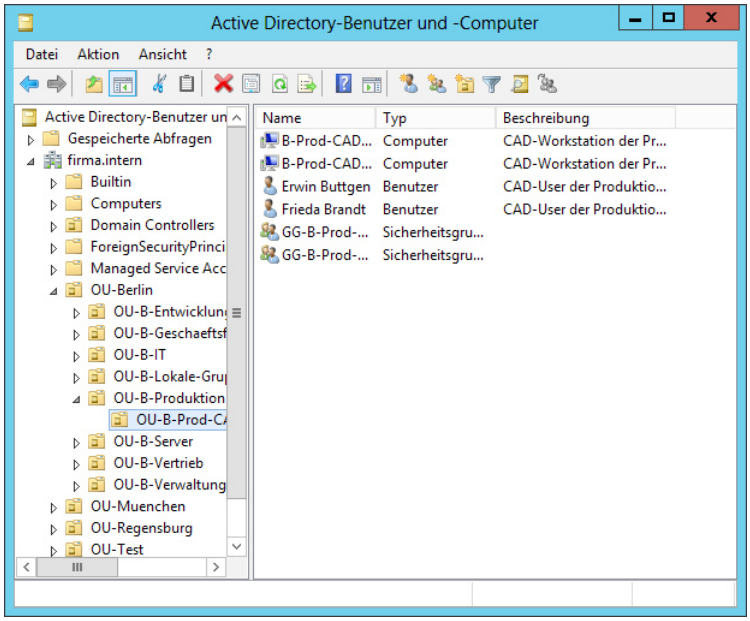

Bild 3.16 OU-Struktur der Beispielfirma

Sie möchten nun die in Tabelle 3.1 dargestellten Einstellungen mittels Gruppenrichtlinien realisieren.

Tabelle 3.1 Anforderungen für Gruppenrichtlinien

▪ Kennwörter sollen mindestens neun Zeichen lang sein und müssen den Komplexitätsanforderungen entsprechen.
▪ Alle Rechner sollen einen lokalen WSUS-Server für die Verarbeitung von Softwareupdates verwenden. Dies betrifft auch die mobilen Rechner.
▪ Standardbenutzer dürfen die Bildschirmauflösung nicht ändern.
▪ CAD-Benutzer dürfen die Bildschirmauflösung ändern.
▪ Wartungs-Ingenieure dürfen auf alle Funktionen der Systemsteuerung zugreifen. Wartungs-Ingenieure sind zugleich Standardbenutzer der Produktionsabteilung.
▪ Standardsoftware soll an alle Benutzer der Produktionsabteilung verteilt und auf jedem Rechner installiert werden, an dem sich die Benutzer anmelden.
▪ Softwareverteilung der Produktionssoftware soll nur an Produktionsserver erfolgen, nicht an andere Rechner der Produktionsabteilung.

3.5.1 Kennwortrichtlinie

Kennwortrichtlinien greifen nur für Domänenkonten, wenn sie in einer Gruppenrichtlinie auf Domänenebene konfiguriert sind. Darum muss die Einstellung entweder in der Default Domain Policy angepasst werden, oder Sie müssen eine weitere GPO auf der Domäne einrichten, die nach der Default Domain Policy verarbeitet wird.

HINWEIS: Es gibt zwar auch die Möglichkeit, über Kennwort-Einstellungsobjekte (Password Settings Objects, PSOs) Kennwortregeln zu definieren, diese sind jedoch keine Gruppenrichtlinien und sollen an dieser Stelle nur der Vollständigkeit halber erwähnt werden.

3.5.2 Lokaler WSUS

Damit Rechner ihre Updates von einem lokalen WSUS-Server beziehen, müssen Sie zwei Richtlinien für die unterschiedlichen Standorte Berlin und München verwenden. Da zusätzlich mobile Rechner im Einsatz sind, dürfen die Richtlinien nicht auf Organisationseinheiten angewendet werden, sonst müsste man die Computerkonten der mobilen Rechner bei jeder Verlagerung des Benutzers zwischen den Organisationseinheiten verschieben. Hier bieten sich stattdessen zwei Standortrichtlinien an. Bezieht nun ein mobiles Gerät über den lokalen DHCP-Server eine zum Standort passende IP-Adresse, wird vom Active Directory automatisch auch der Standort ermittelt, und die passende Gruppenrichtlinie kann angewendet werden.

3.5.3 Bildschirmauflösung Standardbenutzer

Damit Standardbenutzer der Produktion die Bildschirmauflösung nicht ändern können, wird eine Gruppenrichtlinie definiert, die entsprechende Einstellungen für die Benutzer sperrt. Diese wird mit der OU OU-B-Produktion verknüpft. Entsprechend wird für München verfahren.

3.5.4 Bildschirmauflösung CAD-Benutzer

Die Benutzerkonten der CAD-Benutzer sind in einer untergeordneten Organisationseinheit OU-B-Prod-CAD. In dieser wird die Sperrung der Systemsteuerungselemente für die Bildschirmauflösung aufgehoben. Da die Richtlinie der Unter-OU später verarbeitet wird, werden die entsprechenden Einstellungen der übergeordneten Richtlinie überschrieben. Würde stattdessen die Richtlinienvererbung für die OU-B-Prod-CAD deaktiviert, so erhielten die Benutzer auch andere benötigte Einstellungen nicht.

3.5.5 Wartungs-Ingenieure

Damit die rigiden Einstellungen der GPO für Benutzer der Produktionsabteilung nicht die Wartungs-Ingenieure behindern, muss ihnen das Übernehmen der Gruppenrichtlinie für Produktionsbenutzer verweigert werden. Andere Richtlinien der OU sollen trotzdem für sie gelten.

3.5.6 Softwareverteilung Produktionsbenutzer

Standardsoftware soll für alle Benutzer der Produktionsabteilung installiert werden. Da die Installation nur erfolgt, wenn ein Benutzer sich erstmalig an dem Rechner anmeldet und dieser anschließend neu startet, stellen die mobilen Rechner hierbei kein Problem dar, und die Richtlinie kann an die OU-B-Produktion (respektive OU-M-Produktion) mit dem passenden lokalen Pfad zur Installations-Freigabe erfolgen.

HINWEIS: Dies ist ein Grund, warum man die Vererbung der OU-B-Prod-CAD nicht deaktivieren darf. Die Richtlinie würde sonst nicht auf die CAD-Benutzer angewendet werden.

3.5.7 Softwareverteilung Produktionsserver

Da die Spezialsoftware nur auf ausgewählten Computern installiert werden soll, könnte man hierzu mit einer positiven Sicherheitsfilterung gewährleisten, dass nur die Gruppe Produktionsserver die Richtlinie anwenden darf. Hierzu würde man die Authentifizierten Benutzer entfernen und stattdessen eine entsprechende Sondergruppe einsetzen.

3.6 Loopbackverarbeitungsmodus

Es gibt Sonderfälle, in denen die Verarbeitung einer Gruppenrichtlinie für die Benutzerkonfiguration nicht in Abhängigkeit vom Speicherort des Benutzerobjektes erfolgen soll. Um dies zu verdeutlichen, soll das folgende Beispiel dienen.

Ein Mitarbeiter der Produktionsabteilung soll zu einem Wartungs-Ingenieur weitergebildet werden. Zu Übungszwecken meldet er sich an einem Testsystem an. Wenn er an diesem Rechner arbeitet, soll er Zugriff auf die Systemsteuerung haben. Weil er aber die Zertifizierungsprüfung noch nicht bestanden hat, darf er an Produktivsystemen noch nicht auf die Systemsteuerung zugreifen.

3.6.1 Zusammenführen-Modus

In diesem Fall kann man das Testsystem in einer eigenen OU platzieren und für diese die Loopback-Verarbeitung im Modus „Zusammenführen“ aktivieren. Dies bedeutet, dass nach der normalen Verarbeitung von Gruppenrichtlinien eine zweite Verarbeitung des Bereichs Benutzerkonfiguration für den Speicherort des Computerkontos erfolgt. Somit gelten letztendlich andere Einstellungen als für den Benutzer an anderen Rechnern.

3.6.2 Ersetzen-Modus

Sollen stattdessen alle Richtlinien der Benutzerkonfiguration nur unter Berücksichtigung des Speicherortes des Computerkontos ausgewertet werden, kann man den Modus „Ersetzen“ verwenden. Dies bietet sich z. B. an, wenn ein Rechner für eine Online-Prüfung in einen besonders sicheren Modus versetzt werden soll, damit der Prüfungskandidat nur die erlaubte Software ausführen kann.

3.6.3 Loopbackverarbeitungsmodus einrichten

Öffnen Sie die GPO mit dem Gruppenrichtlinienverwaltungs-Editor, indem Sie im Kontextmenü auf BEARBEITEN klicken. Navigieren Sie nun in der Konsolenstruktur auf COMPUTERKONFIGURATION – RICHTLINIEN – ADMINISTRATIVE VORLAGEN – SYSTEM – GRUPPENRICHTLINIE und wählen Sie im rechten Fenster LOOPBACKVERARBEITUNGSMODUS FÜR BENUTZERGRUPPENRICHTLINIE.

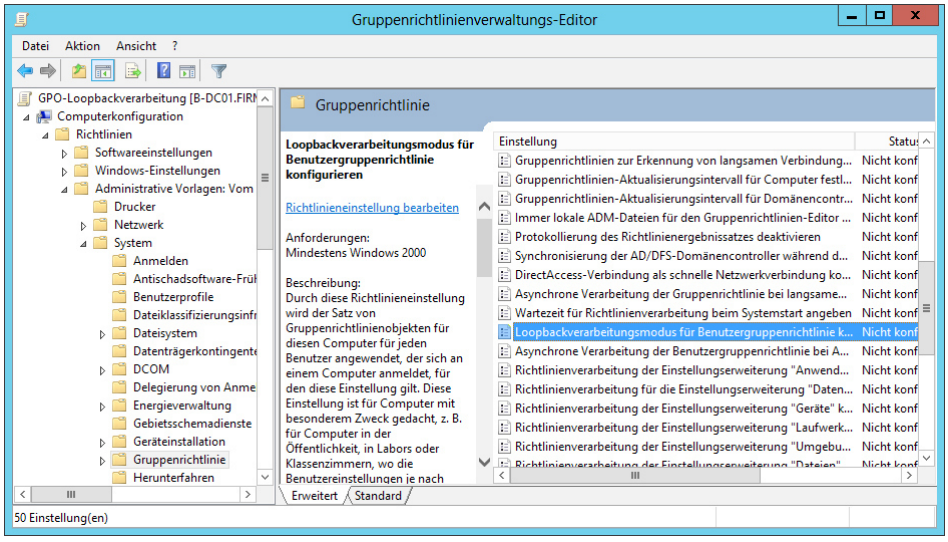

Bild 3.17 Loopbackverarbeitungsmodus aufrufen

Nun können Sie die Richtlinie aktivieren und im Rollfeld den entsprechenden Modus auswählen. Bestätigen Sie anschließend Ihre Konfiguration mit Übernehmen und schließen Sie das Fenster mit OK.

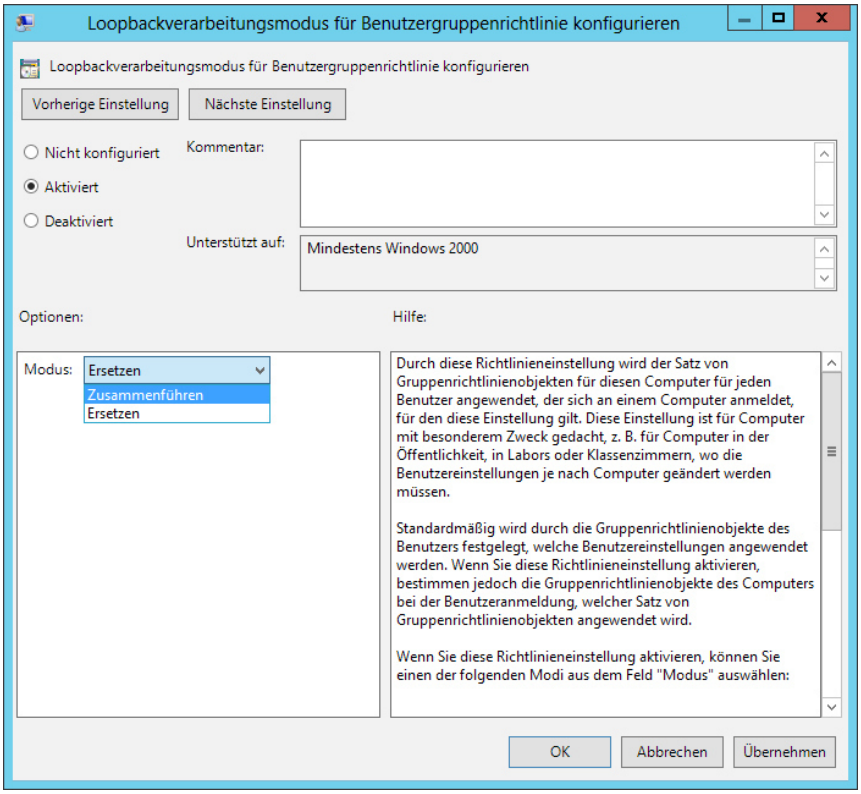

Bild 3.18 Loopbackverarbeitungsmodus aktivieren

Sie können Ihre Konfiguration nun mit der Gruppenrichtlinienverwaltungskonsole überprüfen. Öffnen Sie dazu im rechten Fenster das Register Einstellungen und erweitern Sie die Ansicht mit Klick auf Show.

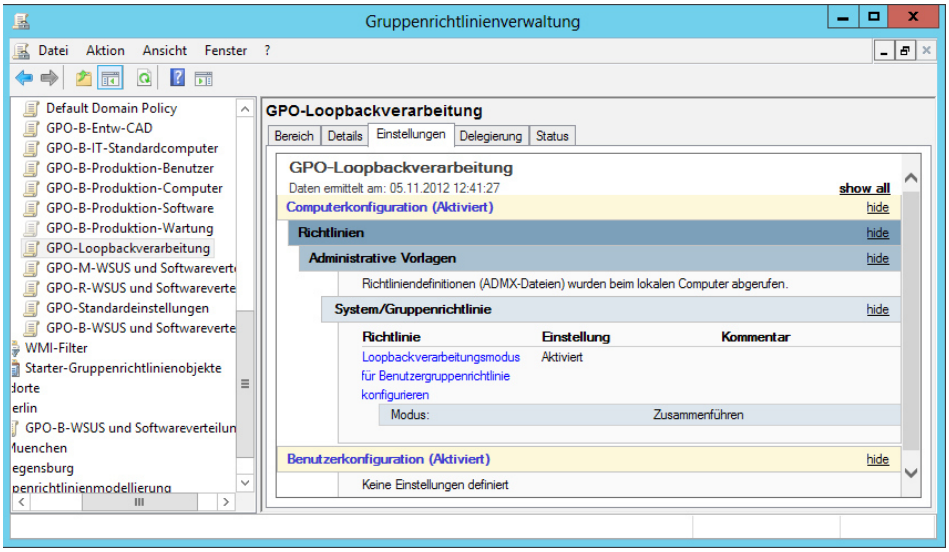

Bild 3.19 Loopbackverarbeitung überprüfen