Unterrichtseinheit 9

Sicherheitsrichtlinien werden verwendet, um die Sicherheit im Netzwerk zu verstärken. Die effizienteste Möglichkeit zum Implementieren dieser, stellt die Verwendung von *Sicherheitsvorlagen* (eine Textdatei, welche Sicherheitseinstellungen enthält, die zum Konfigurieren von Computern mit konsistenten Einstellungen verwendet werden) dar.

Es gibt zwei verschiedene Methoden, um Sicherheitsrichtlinien zu implementieren:

1. Mit Hilfe einer lokalen Systemrichtlinie auf einem einzelnen Computer *(Start→Programme→Verwaltung→Lokale Sicherheitsrichtlinie)*

Achtung: Diese Richtlinie wirkt sich nur auf den **lokalen** Computer aus!

2. Über eine Gruppenrichtlinie in einer Domäne (Gruppenrichtlinien – welche in einen Gruppenrichtlinienobjekt [Group Policy Object, GPO] enthalten und einem Objekt in Active Directory zugeordnet sind - definieren die von einem Systemadministrator verwalteten Komponenten der Desktopumgebung des Benutzers.

Achtung: Diese Richtlinie wirkt sich auf **mehrere** Computer in der Domäne aus!

Implementieren einer lokalen Sicherheitsrichtlinie :

Start → Programme → Verwaltung → Lokale Sicherheitsrichtlinie → Kontorichtlinien → Kennwortrichtlinien

In der lokalen Sicherheitsrichtlinie die Konsole erweitern und auf die zu ändernde Option doppelklicken. In der rechten Hälfte der Konsole können nun die gewünschten Einstellungen getätigt werden. Diese sind eindeutig erklärt und können aktiviert oder deaktiviert werden.

Implementieren von Sicherheit auf mehreren Computern

Erstellt werden Gruppenrichtlinien mit Hilfe der Microsoft Management Console kurz MMC. *(Start→Programme→MMC)*

Detaillierte Anleitung in den MOC Unterlagen Kapitel 9 Übung 1,2,3 oder in der Windows Hilfe unter MMC .

Wichtig: Gruppenrichtlinieneinstellungen werden in der folgenden Reihenfolge übernommen: Zuerst werden **lokale** Einstellungen, dann **Standort- und Domäneneinstellungen** und schließlich **Organisationseinheiteneinstellungen** übernommen.

Ändern der Sicherheitseinstellungen

Folgende Liste beschreibt die Sicherheitseinstellungen, die unter Verwendung der **lokalen Sicherheitsrichtlinie,** oder der Erweiterung für Sicherheitseinstellungen in der **Gruppenrichtlinie** für Computer konfiguriert werden können:

- ***Kontorichtlinien*** Konfigurieren des Kennwortes und der Kontorichtlinien (primäres Sicherheitsprotokoll innerhalb einer Domäne → Kerberos V5)
- ***Lokale Richtlinien*** Konfigurieren der lokalen Überwachung, Benutzerrechte und Sicherheitsoptionen
- ***Richtlinien öffentlicher Schlüssel*** Konfigurieren von Agenten für die Wiederherstellung von verschlüsselten Daten, Domänenstämmen, vertrauenswürdigen Zertifizierungsstellen, etc.
- ***IP-Sicherheitsrichtlinien*** Konfigurieren der IP Sicherheit (Internet Protocol Security, IPSec) in einem Netzwerk und der Kommunikation in einem Intranet, bzw. virtuellen privaten Netzwerk (VPN) über das Internet.

Die folgenden Sicherheitsrichtlinien können nur mit Hilfe der Erweiterung für Sicherheitseinstellungen in der Gruppenrichtlinie konfiguriert werden:

- ***Ereignisprotokoll*** Konfigurieren der Einstellungen für Anwendungs-, System- und Sicherheitsprotokolle
- ***Eingeschränkte Gruppen*** Konfigurieren von Gruppenmitgliedschaften für vordefinierte/sicherheitsgefährdete Gruppen (Administratoren , Domänenadmins usw.) mit bestimmten vordefinierten Funktionen
- ***Systemdienste*** Konfigurieren der Sicherheits- und Starteinstellungen für Dienste, die auf einem Computer ausgeführt werden
- ***Registrierung*** Konfigurieren der Sicherheit für Registrierungsschlüssel
- ***Dateisystem*** Konfigurieren der Sicherheit für bestimmte Dateipfade

Verwenden von vordefinierten Sicherheitsvorlagen

Vordefinierte Vorlagen können häufig einen Startpunkt zum Anpassen einer idealen Sicherheitskonfiguration bereitstellen. Die unter Windows 2000 vordefinierten Sicherheitsvorlagen (ändern die Standardsicherheitseinstellungen inkrementell) wurden entworfen, um allgemeine Sicherheitsanforderungen zu erfüllen. Sie schließen Vorlagen ein, die vier Sicherheitsstufen bieten :

- ***Basis*** (definieren die Standardsicherheitsstufe für W2K)
- ***Kompatibel*** (höhere Sicherheitsstufe als Basis)
- ***Sicher*** (zusätzliche Sicherheitsstufe gegenüber Kompatibel)
- ***Sehr Sicher*** (höchste Sicherheitsstufe für W2K)

Wichtig: Beim Aktualisieren von Computern unter Microsoft WinNT 4.0, welche mit dem NTFS-System laufen, wird die Sicherheit nicht geändert. Sie bleibt jedoch unter der Windows 2000 Sicherheitsstufe Basis.
Falls beim Aktualisieren von WinNT 4.0 auf Windows 2000 die Partition in eine FAT Partition umgewandelt wird, kann die Sicherheit für diesen Computer nicht übernommen werden.

Sicherheitsstufe	***Workstation***	***Server***	***Domänencontroller***
Basis	***Basicwk.inf***	***Basicsv.inf***	***Basicdc.inf***
Kompatibel	***Compatws.inf***		**nicht in diesem Modus**
Sicher	***Securews.inf***		***Securedc.inf***
Sehr Sicher	***Hisecws.inf***		***Hisecdc.inf***

Es wird nicht gewährleistet, das in den Stufen **Sicher** und **Sehr Sicher** (sicherer Server) alle Features der Standardanwendungen ausgeführt werden können.
Die Basis-Vorlagen befinden sich im Ordner ***%SystemRoot%\Security\Templates***

Erstellen von benutzerdefinierten Sicherheitsvorlagen

1. Microsoft Management Console (MMC) starten
2. Snap-In hinzufügen
3. Auswählen der anzupassenden Vorlage (%SystemRoot%\Security\Templates)
4. Konfigurieren der neuen Richtlinieneinstellungen
5. Speichern der neuen Konfiguration

Im Gegensatz zur Verwendung der Grafischen Oberfläche ist es ebenso möglich, die Eingabeaufforderung zum Ausführen der Sicherheitskonfiguration und –analyse mit Hilfe von Skriptdateien zu verwenden. Das Programm, das hierzu verwendet wird ist **SECEDIT.EXE**. Es stellt einige Funktionen bereit (wie beispielsweise das

Aktualisieren einer Sicherheitsrichtlinie), welche auf der grafischen Benutzeroberfläche nicht verfügbar sind.

Folgende Schalter, bzw. Optionen werden bei SECEDIT.EXE auf höherer Ebene ausgeführt:

- **/analyze**
- **/configure**
- **/export**
- **/refreshpolicy** (ermöglicht das Erzwingen eines Gruppenrichtlinienübermittlungsereignisses)
- **/validate** (überprüft die Syntax einer Vorlage)
- **/areas** (bestimmte Bereiche der Sicherheitseinstellungen können konfiguriert und exportiert werden)

Überwachung des Zugriffs auf Systemressourcen

Einführung in die Überwachung

Die Überwachung (nur im NTFS-Systemen möglich) stellt den Vorgang des Nachverfolgens von Benutzer- und Betriebssystemaktivitäten (Ereignisse) auf einem Computer dar. (Eintrag zu dem Ereignis im Sicherheitsprotokoll)

Überwachungseinträge

Ein Überwachungseintrag im Sicherheitsprotokoll enthält folgende Informationen:

- Den ausgeführten Vorgang
- Den Benutzer, der den Vorgang ausgeführt hat
- Erfolg oder Fehlschlag und den Zeitpunkt des Ereignisses
- Weitere Informationen, wie z.B. der Computer auf dem das Ausführen des Vorgangs ausgeführt/versucht wurde

Überwachungsrichtlinie

Eine Überwachungsrichtlinie definiert die Typen von Sicherheitsereignissen, die Windows 2000 im Sicherheitsprotokoll auf jedem Computer protokolliert. Windows 2000 schreibt die Ereignisse in das Sicherheitsprotokoll auf dem entsprechenden Computer, auf dem das jeweilige Ereignis aufgetreten ist.

Anzeigen von Ereignissen

Die Konsole **Ereignisanzeige** wird verwendet, um die von Windows 2000 im Sicherheitsprotokoll aufgezeichneten Ereignisse anzeigen zu lassen. Protokolldateien können auch archiviert werden, um Trends über einen längeren Zeitraum nachzuverfolgen. Protokolldateien werden mit der Dateiendung **.evt** (Eventlog) abgespeichert.

Folgende Ereignisse können überwacht werden :

- ***Anmeldeversuche*** z.B. das Anmelden eines Benutzers wird in der Kategorie Kontoanmeldung protokolliert
- ***Kontenverwaltung*** erstellen, umbenennen, aktivieren oder deaktivieren eines Kontos; Kennwort festlegen oder ändern
- ***Active Directory Zugriffe*** Ein Benutzer erhält Zugriff auf ein Active Directory Objekt
- ***Anmeldeereignisse*** An- und Abmelden eines Benutzers, Herstellen einer Netzwerkverbindung; wird auf dem Computer, auf den der Benutzer zugreift, protokolliert (unabhängig davon, ob dieser ein lokales- oder ein Domänenkonto verwendet)
- ***Objektzugriffsversuche*** Benutzer erhält Zugriff auf eine Datei, Ordner usw.
- ***Richtlinienänderung*** Änderung an den Sicherheitsoptionen, Benutzerrechten oder Überwachungsrichtlinien
- ***Rechteverwendung*** Benutzer nimmt ein Recht war: z.B. ändern der Systemzeit, oder Administrator übernimmt die Besitzrechte für eine Datei
- ***Prozessverfolgung*** Eine Anwendung führt einen Vorgang aus
- ***Systemereignisse*** Neustart oder Herunterfahren des Rechners, oder es ist ein Ereignis aufgetreten, das sich auf die Sicherheit von Windows 2000 oder auf das Sicherheitsprotokoll auswirkt

Planen einer Überwachungsrichtlinie

Werden zu viele Ereignistypen überwacht, so kann dies zu einer erheblichen Überlastung und somit auch zu einer Verringerung der Systemleistung führen. Daher sollten nur wirklich nützliche Informationen für die Sicherheitsmaßnahmen überwacht werden.

Zum Planen einer Überwachungsrichtlinie sollte folgendes beachtet werden:

- Bestimmung der zu überwachenden Computer
- Bestimmung der zu überwachenden Ereignisse
- Bestimmung, ob Erfolg oder Fehlschlag (oder beides) überwacht werden soll
- Bestimmung, ob Trends nachverfolgt werden müssen
- Regelmäßige Überprüfung der Sicherheitsprotokolle

Einrichten einer Überwachungsrichtlinie

1) Erstellung einer MMC-Konsole und einfügen des Snap-In`s **Gruppenrichtlinie**. **Lokaler Computer** wird als Gruppenrichtlinienobjekt ausgewählt.
2) Erweitern der Option **Computerkonfiguration** unter **Richtlinien für lokaler Computer → Windows-Einstellungen → Sicherheitseinstellungen → Lokale Richtlinien → Überwachungsrichtlinien**

Achtung: Um eine Überwachungsrichtlinie konfigurieren zu können, muss man Mitglied der Gruppe Administratoren sein!