

Übung 1 : Passwortsicherheit

1. Alternativer Administrator

Zweck: Mit diesem Konto können Sie sich anmelden, wenn es mit dem originären Administratorkonto Probleme gibt, z.B. weil es wegen zu vieler Fehlversuche gesperrt wurde. Es sollte in keinem System fehlen.

Durchführung: Sie finden das Administratorkonto in der ADS in der OU „Users“. Klicken Sie mit der rechten Maustaste auf dieses Konto, wählen Sie kopieren. Sie sollten einen nicht zu erratenden Anmeldenamen und ein kryptisches Passwort wählen. Beides könnten Sie auch in einem versiegelten Umschlag im Schultresor hinterlegen (man weiß ja nie...)

2. Sperrung nach 3-5 Fehlversuchen

Wird über eine Gruppenrichtlinie festgelegt, und zwar auf Domänenbasis (geht nur dort).

ADS – rechte Maustaste auf Domäne – Eigenschaften – Reiter Gruppenrichtlinie – neue anlegen – bearbeiten -

Computerkonfiguration - Windows-Einstellungen – Sicherheitseinstellungen – Kontorichtlinien – Kontosperrungsrichtlinien - Kontosperrungsschwelle aktivieren mit 3-5 Versuchen; Kontosperrdauer in Minuten, z.B. 90; Zurücksetzungsdauer 20min.

3. Loggen der Anmeldeversuche und Blick ins Sicherheitsprotokoll

Über eine Gruppenrichtlinie kann veranlasst werden, dass die Anmeldeversuche in das Ereignisprotokoll des Servers protokolliert werden. Diese Gruppenrichtlinie muss der OU Domain Controllers zugeordnet sein (z.B. die Default DC Policy).

Bearbeiten – Computereinstellungen – Windows-Einstellungen – Sicherheitseinstellungen – Lokale Richtlinien – Überwachungsrichtlinie – Anmeldeereignisse überwachen – erfolgreiche&fehlgeschlagene (nicht: Anmeldeversuche).

Aufruf der Ereignisanzeige über Programme-Verwaltung oder Start-ausführen-eventvwr.msc. Sicherheitsprotokoll ansehen.

Bemerkung: es dauert 15-30min, bis die Gruppenrichtlinie greift.

Übung 2 : Berechtigungen

1. Berechtigungen auf das Stammverzeichnis des Systemlaufwerks

Es ist ein bekannter Fehler von Windows 2000 (in XP behoben!), dass nach der Installation jeder Vollzugriff in diesem Verzeichnis hat.

Abstellen über eine Gruppenrichtlinie in Workstations.

Computereinstellungen – Windows-Einstellungen – Sicherheitseinstellungen – Dateisystem – rechte Maustaste – Datei hinzufügen – Administratoren & System Vollzugriff, Benutzer: lesen, ausführen. OK. Verwenden Sie die oberen Optionen (an..übermitteln), damit die anderen Einstellungen erhalten bleiben. Testen Sie das Ergebnis.

2. Sperren Sie den Zugriff auf c:\winnt\net.exe

Gehen Sie wie in 1. vor, geben Sie aber nur Administratoren und System die Rechte. Benutzen Sie nie verweigern für die Gruppe „jeder“, das betrifft auch die Admins.

3. Das Anlegen von Verknüpfungen verhindern

Mit Verknüpfungen wird das Sicherheitssystem teilweise ausgehebelt. Das Anlegen von Links lässt sich nicht grundsätzlich verhindern, allerdings kann man diese unbrauchbar machen. Dazu muss man der Schülergruppe („g_schueler“) analog wie in 1., aber diesmal in der Registry, den Zugriff auf HKEY_CLASSES_ROOT/.lnk/.shellNew verweigern. Ausprobieren!

Hinweise:

- Analog kann man auch Schreibzugriffe in Ordner oder auf Registryschlüssel zulassen.
- Die Gruppenrichtlinien greifen erst nach einem Neustart des Clients (oder nach 2 Stunden Wartezeit)
- Zum Testen kann man auch Start-Ausführen-secedit /refreshpolicy MACHINE_POLICY eingeben.
-

Übung 3 : SUS-Server

Bitte gehen Sie nach der Anleitung von www.support-netz.de vor.

Hinweis für ML 1.5 (Windows 2003): das lockdown-Tool müssen Sie hier nicht mehr einsetzen. W2k3 verwendet schon standardmäßig geeignete Sicherheitseinstellungen.

Links zum Thema:

<http://www.bsi.bund.de/gshb/deutsch/m/m04148.html>

<http://www.ipworks.de/files/logonoff.doc>

http://www.gruppenrichtlinien.de/HowTo/SUS_Server.htm

<http://winmuster.shellmaster.de/cms/Musterloesung/detail.php?nr=215&kategorie=Musterloesung>

<http://winmuster.shellmaster.de/cms/Musterloesung/detail.php?nr=174&kategorie=Musterloesung>