# Hardening Checkliste

# Windows 2003 Intranet Basis

# 30. November 2004

| | |
|---|---|
| Name des Dokument: | Checkliste_Win2K3_Intranet_Basis_V1.7.doc |
| Version: | V 1.7 |
| Autor: | Christoph Schnidrig, Compass Security AG |
| Erstellungsdatum: | 28. Mai 2003 |
| Anpassungsdatum: | 30. November 2004 |
| Lizenznehmer: | Company Name |

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

# Inhaltsverzeichnis



GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

# 1 Übersicht

## 1.1 Audienz

Diese Checkliste richtet sich an technische Sachverständige. Grundwissen im Bereich von Windows 2003 wird vorausgesetzt.

## 1.2 Dokumentstruktur

| Kapitel | Inhalt |
|---|---|
| 1 | Übersicht über dieses Dokument. |
| 2 | Einführung in das Vorgehen beim Hardening |
| 3 | Vorschläge zur Planung |
| 4 | Hardening-Massnahmen für Domänen |
| 5 | Hardening-Massnahmen für Member Server |
| 6 | Hardening-Massnahmen für Domänen Kontroller |
| 7ff | Anhang |

## 1.3 Weitere Checklisten

Compass Security bietet nebst dieser Hardeninganleitung folgende verwandte Listen an. Alle diese Listen sind für Intranet-Systeme optimiert. Wenden Sie sich bei Interesse an info@csnc.ch.

| Hardeninganleitung | Beschreibung |
|---|---|
| Windows 2003 Intranet Basis | Hardeningempfehlungen für Memberserver, Domaincontroller sowie ADS. |
| Exchange 2003 | Hardeningempfehlungen für Exchange 2003 Server. Vorausgesetzt wird das Hardening des Betriebsystems (siehe Intranet Basis Liste) |
| SQL 2003 | Hardeningempfehlungen für SQL 2003 Server. Vorausgesetzt wird das Hardening des Betriebsystems (siehe Intranet Basis Liste) |
| Internet Information Server 6.0 for Intranet | Hardeningempfehlungen für IIS 6.0 Server. Vorausgesetzt wird das Hardening des Betriebsystems (siehe Intranet Basis Liste) |

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

| Hardeninganleitung | Beschreibung |
|---|---|
| Windows XP Professional | Hardeningempfehlungen für domänenzugehörige Workstations mit Windows XP Proffessional |
| ISA 2004 | Hardeningempfehlungen für ISA 2004 Server. Vorausgesetzt wird das Hardening des Betriebsystems (siehe Intranet Basis Liste) |

## 1.4 Versionskontrolle

| Version | Datum | Änderungen | Autor |
|---|---|---|---|
| 1.0 | 28.05.2003 | Erste Version | Christoph Schnidrig |
| 1.1 | 22.08.2003 | • Kapitel 2.3.2, 7.1 und 7.2 eingefügt<br>• Neue Group Policy Management Console beschrieben<br>• Nummerierung der Punkte angepasst<br>• SNMP Service Einstellungen geändert | Christoph Schnidrig |
| 1.2 | 17.09.2003 | • Terminal Services Hardening erweitert. Siehe Kapitel 5.9<br>• Setzen des lokalen Admin Passwortes. Siehe Kapitel 5.2<br>• Zu installierende Hotfixes. Siehe Kapitel 7.4<br>• Einge Bugs im Dokument gefixt | Christoph Schnidrig |
| 1.3 | 13.11.2003 | • Diverse textuelle Anpassungen<br>• Erneuerung der Top10 Liste. Siehe Kapitel 2.3.5<br>• Neusortierung der Empfehlungen<br>• Aktualisierung der relevanten Patches. Siehe Kapitel 7.4<br>• Update des Kapitels 5.1 | Christoph Schnidrig |
| 1.4 | 18.11.2003 | Lizenznehmer im Seitenkopf eingefügt. | Jan P. Monsch |
| 1.5 | 06.01.2004 | Fehler in der Dokumentenstrukturtabelle behoben. | Jan P. Monsch |

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

| Version | Datum | Änderungen | Autor |
|---|---|---|---|
| 1.6 | 28.01.2004 | • Empfehlungen bezüglich Policy Tests eingefügt. Siehe Kapitel 2.3.4<br>• Default Policies können entfernt werden. Siehe Kapitel 7.1.3.3<br>• Hinweis bezüglich des Imports der INF-Files bei DC's. Siehe Kapitel 3.2<br>• Diverse Einstellugen geändert<br>• NT4 Compliance eingearbeitet. Siehe Kapitel 2.3.1 und 7.6<br>• Tool für automatische Patchchecks. Siehe Kapitel 7.4.1<br>• Zu installierende Hotfixes. Siehe Kapitel 7.4 | Christoph Schnidrig |
| 1.7 | 18.11.2004 | • Neue Checkliste verfügbar (ISA 2004)<br>• Top10 Windows Schwachstellen aktualisiert<br>• Abgleich mit der Default Policy, zusätzlich entsprechende Einstellung eingefügt | Christoph Schnidrig |

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

# 2 Einführung

## 2.1 Disclaimer

Im folgenden ein Auszug aus den Vertragsvereinbarungen zwischen dem Kunden und Compass bezüglich Gewährleistung und Haftung:

**Compass gewährleistet, dass der Vertragsgegenstand sämtlichen Compass zum Zeitpunkt des Vertragsschlusses bekannten technischen Standards entspricht.**

**Compass übernimmt jedoch keinerlei Gewähr dafür,**

- **dass der Vertragsgegenstand fehlerfrei ist;**
- **dass durch den Einsatz des Vertragsgegenstandes sämtliche Angriffsmöglichkeiten in das System des Kunden ausgeschlossen werden;**
- **dass das System des Kunden nach dem Einsatz des Vertragsgegenstandes in jedem Falle einwandfrei funktioniert.**

**Compass lehnt sodann jede Gewährleistung ab, falls der Kunde den Vertragsgegenstand entgegen ausdrücklichen Anweisungen von Compass eingesetzt hat.**

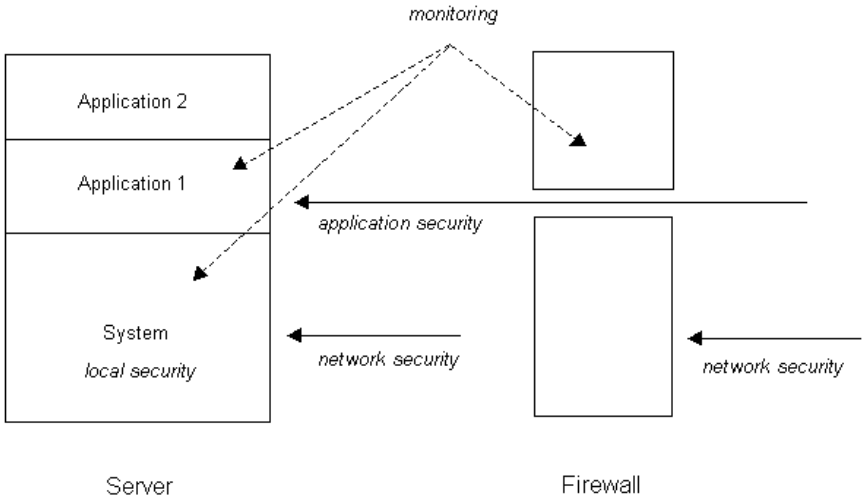
**Compass lehnt jede Haftung für direkte oder indirekte Schäden, die beim Einsatz des Vertragsgegenstandes entstanden sind, ab. Vorbehalten bleiben Fälle, bei denen Compass Absicht oder Grobfahrlässigkeit nachgewiesen werden kann.**

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

## 2.2 Lokale-, Netzwerk- und Applikationssicherheit

Um ein Netzwerk sicher zu konfigurieren müssen folgende Stufen betrachtet werden. Diese Stufen beschreiben die verschiedenen Problembereiche, welche von Hackern angegriffen werden.




| Stufe | Definition | Gegenmassnahmen |
|---|---|---|
| Lokale Sicherheit | Der Angreifer hat bereits Zugriff auf das System. Nun versucht er seine Privilegien zu erweitern. (Local Exploits) | Hardening<br>Patchen |
| Netzwerk Sicherheit | Der Angreifer hat noch keinen Zugriff auf dem Opfersystem. Nachdem scannen versucht er Schwachstellen auszunutzen um Zugriff zu erlangen. (Remote Exploits) | Hardening<br>Firewall |
| Applikationssicherheit | Der Angreifer sucht den Zugriff auf eine E-Business Applikation. Findet er diesen versucht er die Daten eines anderen Benutzers einzusehen. | Sicherheitsbewusste Entwicklung von Webapplikationen |
| Überwachung | Analyse (automatische wie auch manuelle) der Logfiles und des Netzwerkverkehrs. | Loganalyse Tools<br>Intrusion Detection Systeme |

## 2.3 Hardening (Get Secure)

Standardinstallationen bergen eine Unmenge von sicherheitstechnischen Problemen. Die Ursachen dazu sind:

- Rückwärts Kompatibilität
- Funktionalität

Hinzu kommen weitere Sicherheitslücken, die von Administratoren und Benutzern während dem Betrieb geschaffen werden:

- Schlechte Rechtevergabe
- Schwache Passwörter
- Sicherheitstechnisch schwache Konfigurationen
- Veralteter Patchlevel
- usw.

Man sieht eine Unmenge von Bereichen die von Hackern ausgenutzt werden können. Brisant ist, dass auch ein „Nichts tun“ Probleme verursachen kann (z.B. Installation des neusten Servicepacks).

Um ein neu installiertes System auf einen sicheren Stand zu bringen, wird es einem Hardening unterzogen. Beim Hardening werden unter anderem die oben genannten Punkte angegangen. Dabei erscheinen die einzelnen Schritte als unnötig. Die Güte von Sicherheit kann mittels Anreihung von Hürden definiert werden. Jede noch so kleine Hürde ist eine weitere Massnahme, die den Weg eines Angreifers erschwert resp. versperrt.

### 2.3.1 Umfeld

Diese Checkliste wurde für die Zusammenarbeit mit folgenden Betriebsystemen entwickelt:

- Windows 2003 Domain im Native Mode
- Windows XP, 2000 und NT Workstations
- Windows 2003, 2000, und NT Member Server

Im Anhang ist ein Kapitel (siehe 7.6) eingefügt, welches die Einstellungen auflistet, die zusätzlich ein- resp. ausgeschaltet werden können, wenn keine NT4 Computer mehr benutzt werden.

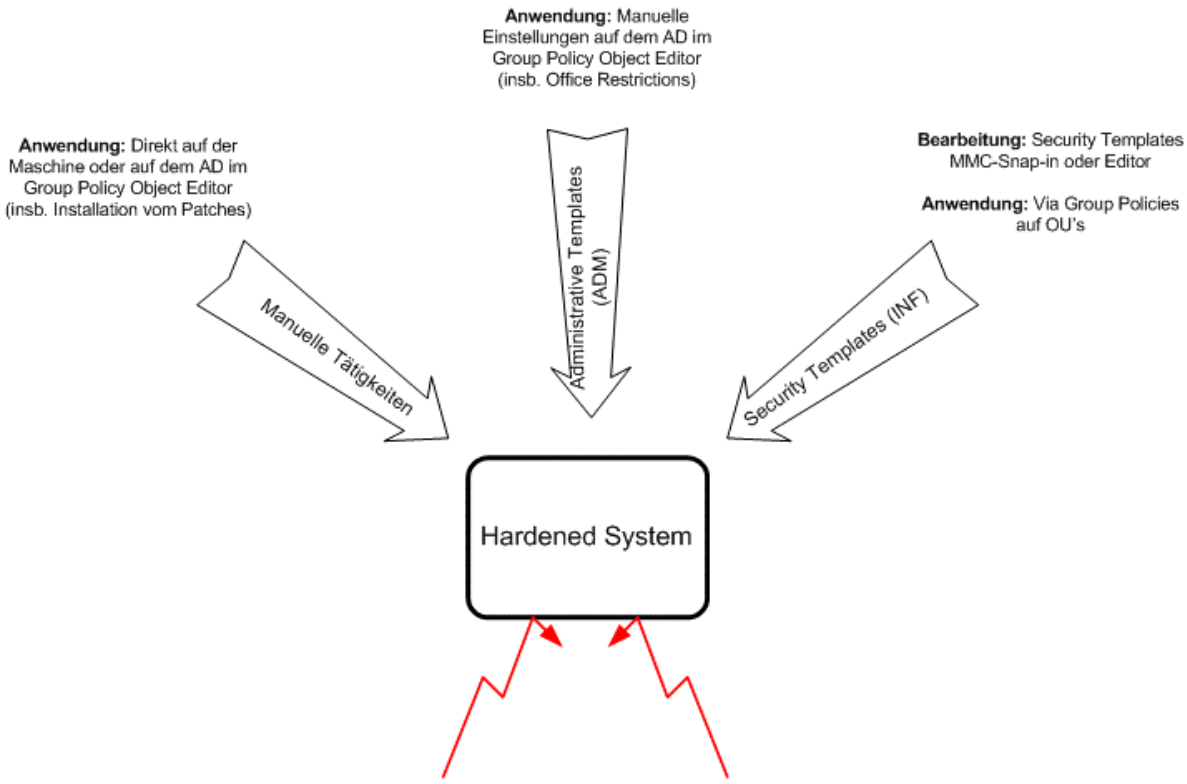
GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

### 2.3.2 Übersicht

Untenstehende Abbildung illustriert die verschiedenen Tätigkeiten, welche in dieser Hardeninganleitung beschrieben werden.

- Leider können nicht alle Einstellungen automatisiert angewendet werden. Im „Group Policy Object Editor“ sind diejenigen Einstellung die nicht unter „Windows Settings-Security Settings“ gemacht werden können, manuell einzugeben.
- Die meisten Settings unter „Windows Settings-Security Settings“ können automatisiert und einfach mittels einer INF-Datei eingelesen werden.
- Der Import von ADM-Dateien erweitern die Einstellungsmöglichkeiten unter „Administrative Templates“. So können umfangreiche Einstellungen auf dem Client einfach über die ganze Firma verteilt werden.




GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

### 2.3.3 Vorgehen

Weil beim Hardening oftmals die Funktionalität gegen Sicherheit ersetzt wird, können vielseitige und komplexe Probleme auftreten. Wenn nicht genau verstanden wird, was welche Einstellung bezweckt und blind einer Checkliste gefolgt wird, könnten Applikationen den Dienst quittieren. Deshalb ist es wichtig das Hardening auf das entsprechende Unternehmungsnetzwerk anzupassen.

**Obwohl die vordefinierten Sicherheitsvorlagen (.inf-Dateien) zu einem zügigen Vorgehen einladen, wird dringend empfohlen, die in dieser Checkliste aufgeführten Punkte durchzugehen und zu hinterfragen.**

Folgende Punkte sollten bei einem Hardening beachtet werden:

- Adaption von Empfehlungen auf das eigenen Unternehmensnetzwerk
- Strukturiertes Vorgehen in Teilschritten
- Vorgängiges Überprüfen (Testumgebung)
- Dokumentation von geprüften Konfigurationen (Sicherstellen der Wiederverwendbarkeit)

Hilfestellungen bei Problemen:

- Einkreisung des Problems
- Was könnte dieses Problem verursachen (Vergleich mit der Checkliste)
- **Strukturierte** Suche und „Unhardening“ in Teilschritten (Achtung: Keine zusätzliche Sicherheitsprobleme schaffen wie z.B. Zuordnung von Administrator-Rechten oder Everyone-Zugriffen)
- Eventlogs und Fehlermeldungen auswerten und in der TechNet Knowledgebase nach Lösungen suchen

### 2.3.4 Policy Test

Es wird dringend empfohlen die neu erstellten Policies zu testen. Dies kann im Rahmen einer Testumgebung geschehen. Auch wird empfohlen die Policies nicht gleich auf alle Server zu applizieren. Es sollen eigene Test-OU’s erstellt werden, auf welche die Policies in einem ersten Schritt angewendet werden. Danach werden einzelne Server resp. Workstations in die Test-OU’s verschoben. So kann die Policy zuerst getestet werden bevor diese in die produktive Umgebung installiert wird.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

### 2.3.5 Top Schwachstellen bei Windows Systemen

Die grosse Mehrheit von erfolgreichen Attacken nützt eine kleine Anzahl von Schwachstellen aus. Es wird immer der Weg des geringsten Widerstandes gesucht. Oftmals existieren für solche Schwachstellen einfache Tools, die von jedem „Hobbyhacker“ angewendet werden können. Werden auf dieser Basis Würmer gebaut resultieren daraus fatale Folgen.

SANS hat in Zusammenarbeit mit dem FBI eine Liste zusammengestellt, in welcher auf die grössten und meist ausgenutzten Schwachstellen für Unix und Windows hingewiesen wird. Untenstehend sind die entsprechenden Punkte für Windows Systeme abgedruckt.

http://www.sans.org/top20/

| # | Schwachstelle | Gegenmassnahmen |
|---|---|---|
| 1 | Web Servers & Services | Hardening<br>Regelmässiges Patchen |
| 2 | Workstation Service | Hardening<br>Regelmässiges Patchen |
| 3 | Windows Remote Access Services | Hardening (Kapitel 5.5) |
| 4 | Microsoft SQL Server (MSSQL) | Hardening<br>Regelmässiges Patchen |
| 5 | Windows Authentication | Hardening (Kapitel 5.5) |
| 6 | Web Browsers | Hardening (Kapitel 5.9)<br>Regelmässiges Patchen<br>Proxy mit Content Filter und Virenscanner |
| 7 | File-Sharing Applications | Interne Richtlinien sollten den Gebrauch solcher Software verbieten. Firewall sollte die benutzen Protokolle blocken. |
| 8 | LSAS Exposures | Firewallregeln<br>Regelmässiges Patchen |
| 9 | Mail Client | Deinstallation von Outlook Express. Hardening von Outlook gemäss Kapitel 5.1. |
| 10 | Instant Messaging | Deinstallation von Messenger (Kapitel 5.1)<br>Firewallregeln<br>ActiveX verbieten (Kapitel 5.9) |

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

# 3 Planung

## 3.1 Berechtigungen

Auf Berechtigungen auf Freigabeebene wird hier nicht genauer eingegangen. Es möchte hier nur auf folgende goldene Regel der Sicherheit aufmerksam gemacht werden.

**Least Privilege Prinzip - Genau soviel wie nötig**

So kann nicht nur Datenklau und unberechtigter Dateneinsicht verhindert werden, sondern auch der Wirkungskreis von Viren eingegrenzt werden. z.B. Iloveyou (Loveletter Virus) überschrieb viele Dateien – auch auf gemappten Laufwerken.

### 3.1.1 Domain Trust Schwachstelle

Es möchte hier auf eine bekannte Schwachstelle in Windows 2000 und 2003 aufmerksam gemacht werden. Es ist jedem Benutzer, der mit administrative- oder Backup/Restore-Rechten auf einer Domäne innerhalb eines Forest ausgestattet ist, möglich auf dem gesamten Domänenverbund Adminrechte zu erlangen. Dazu gibt es keinen Patch, tief greifende Änderungen im Design vom Active Directory wären nötig diese Schwachstelle zu stopfen. Jedoch muss der Angreifer über ein relativ grosses Know-how verfügen und es bleibt in Frage gestellt ob er den gewünschten Zugriff nicht einfacher erreichen könnte.

Weiterführende Informationen zu dieser Schwachstelle:

http://www.microsoft.com/technet/security/bulletin/MS02-001.asp
http://www.aelita.com/solutions/ADSecurity/SIDH_implications.htm

## 3.2 OU-Plan

Mittels Organisationseinheiten (Organizational Unit) werden Objekte im Active Directory organisiert. Gleiches wird dabei gruppiert. Es handelt sich dabei um:

- Benutzer
- Computer
- Drucker
- andere OUs

OUs werden für folgende Tätigkeiten eingesetzt:

- Delegieren der Verwaltung an AD-Objekte (Admin Gruppen Rechte zuweisen)
- OUs sind keine sind keine Sicherheitsprinzipals → Organisieren von Ressourcen, nicht Festlegen von Berechtigungen (Dies wird über Gruppen bewerkstelligt)
- Gruppenrichtlinien wird auf OU Gruppenrichtlinien festgelegt

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

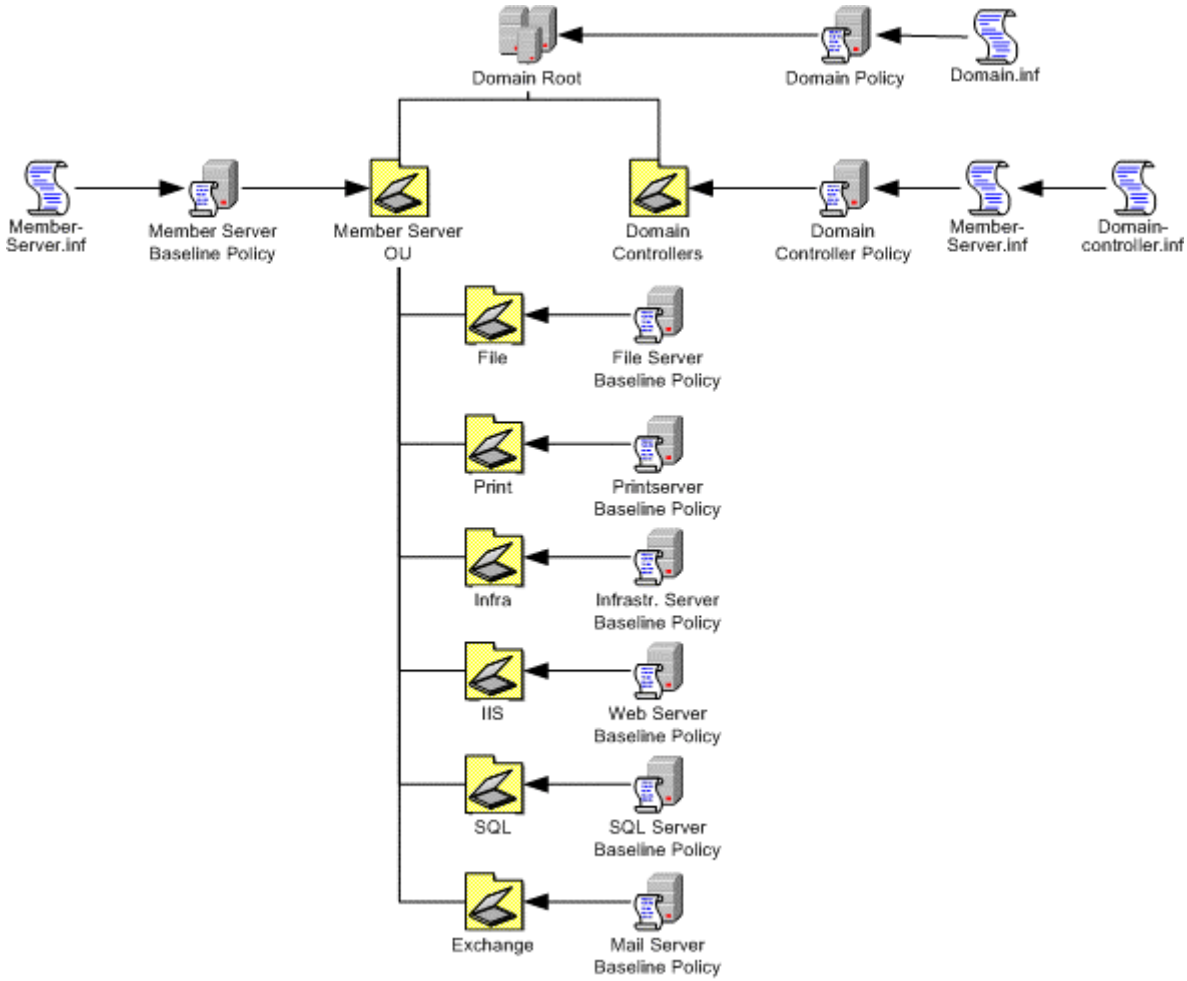
- OUs sind für die Verwaltung bestimmt und für Benutzer unsichtbar

Wie nun die OU Struktur festgelegt wird, muss im Einzelnen entschieden werden. Rudimentär betrachtet müssen folgende Punkte beachtet werden (untenstehende Aufteilung soll lediglich als Beispiel betrachtet werden):

- Erstellen von OUs zum Delegieren von Verwaltungsaufgaben
  - OUs nach physischen Standort (Vorteilhaft für Drucker und Computer)
  - OUs nach Geschäftsbereich (Geeigneter für Benutzerkonten)
- Erstellen von OUs für die Zuweisung von Gruppenrichtlinien (Security Templates)
  - OUs nach Funktion oder Aufgabe (Benutzer und Server)

Untenstehende Abbildung zeigt ein Beispiel für die Anwendung der Security Templates auf Server auf.

**Achtung:**
Besondere Beachtung gilt es dabei der Domain Controller Policy geschenkt werden. Es muss da zuerst das Member Server INF-File und danach das Domain Controller INF-File importiert werden. Ansonsten werden auf den DC's sämtliche ADS-Dienste gestoppt!




GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

## 3.3 Priorität der Group Policy

Mittels Group Policies können die einzelnen Einstellungen angewendet werden. Da diese Policy einer Gruppe (OU) zugeordnet wird, werden die Einstellungen auf allen Servern in der entsprechenden OU übernommen. Werden neue Objekte in OUs mit aktiven Group Policies verschoben, erhalten diese Objekte automatisch die definierten Einstellungen.
Group Policies können auf verschiedenen Stufen angelegt werden. Folgende Liste zeigt die Reihenfolge der Zuordnung der Policies.

1. Local Policy
2. Site Policy
3. Domain Policy
4. Parent OU Policy
5. Child OU Policy (geschachtelte OU)

→ Werden die gleichen Einstellungen in verschiedenen Stufen festgelegt, entspricht die zu letzt Zugeordnete der effektiven Einstellung.

→ In den Eigenschaften der Group Policy kann die Option „No Override“ angewählt werden. In diesem Fall wird die entsprechende Policy nicht überschrieben.

## 3.4 Security Management (Stay Secure)

Das Hardening und somit die Empfehlungen in diesem Dokument konzentrieren sich auf die Sicherung eines Systems zu einem bestimmten Zeitpunkt. Da im Laufe der Zeit neue Erkenntnisse und Schwachstellen auftauchen, schwindet der Sicherheitslevel. Zudem ist das System selber einem Wandel ausgesetzt. D.h. Software wird installiert und Konfigurationen werden geändert. Aus diesen Gründen ist ein Security Management, welches folgende Tätigkeiten beinhaltet, unablässig.

- Zweckmässiges Logging und Kontrolle der Logs (siehe Anhang)
- Installation und Betrieb eines IDS
- Abonnieren aller relevanten Security Newsletter (siehe Anhang)
- Regelmässige Updates (Hotfixes, Updates)
- Regelmässige Vulnerability Scans im Intranet (z.B. Nessus, LanGuard,…)
- Regelmässige Passwort Audits (z.B. L0pht, Cain,…)

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

# 4 Hardening Domain

| Wirkungskreis | Anwendung | Compass Template Name |
|---|---|---|
| Dieses Kapitel beschreibt die domänenweiten Sicherheitseinstellungen. Diese wird auf jedes System, welches der Domäne oder einer Subdomäne angehört, angewendet. | Die entsprechende INF-Datei wird auf die Root-Domäne angewendet. Siehe Kapitel 7.1. | Intranet_Baseline_Security_Domain_CSNC_V1.1.inf |

Die Werte der standardmässig aktiven Policies sind jeweils aufgeführt. Standardmässig gibt es zwei Policies, eine auf Domänenebene (Default Domain Policy) und eine auf Domain-Controller-Ebene (Default Domain Controller Policy). In der Tabellen wurden folgende Abkürzungen verwendet: DDP = Default Domain Policy, DDCP = Default Domain Controller Policy

## 4.1 Account Policies

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 4100 | Kontosperrdauer | Account Lockout Policy: Account lockout duration<br>30 minutes | 💣 | Security Template (Automatisch) |
| 4101 | Kontosperrungsschwelle<br>DDP: 0 invalid login attempts | Account Lockout Policy: Account lockout threshold<br>5 invalid logon attempts | 💣💣 | Security Template (Automatisch) |
| 4102 | Zurücksetzungsdauer des Kontosperrungszählers | Account Lockout Policy: Reset account lockout counter after<br>30 minutes | 💣 | Security Template (Automatisch) |
| 4103 | Erzwingen einer Kennwortchronik<br><br>DDP: 24 passwords remembered | Password Policy: Enforce password history<br>24 passwords remembered | 💣💣 | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 4104 | Maximales Kennwortalter<br>DDP: 42 days | Password Policy: Maximum password age<br>60 days | 💣 | Security Template (Automatisch) |
| 4105 | Minimales Kennwortalter<br>DDP: 1 day | Password Policy: Minimum password age<br>2 days | 💣 | Security Template (Automatisch) |
| 4106 | Minimale Kennwortlänge<br>DDP: 7 characters | Password Policy: Minimum password length<br>8 characters | 💣 | Security Template (Automatisch) |
| 4107 | Kennwort muss einer gewissen Komplexität entsprechen. Die Passwörter müssen dabei folgende Kriterien erfüllen:<br>• Der Username oder Teile davon sind nicht erlaubt<br>• Kennwort Minimumlänge 6 Zeichen<br>• Drei von den folgenden Zeichenkategorien müssen im Kennwort vorhanden sein: (A-Z, a-z, 0-9, Sonderzeichen)<br>DDP: Enabled | Password Policy: Password must meet complexity requirements<br>Enabled | 💣💣 | Security Template (Automatisch) |
| 4108 | Passwörter sollen nicht mit einer reversiblen Verschlüsselung gespeichert werden.<br>DDP: Disabled | Password Policy: Store passwords using reversible encryption<br>Enabled | 💣💣💣 | Security Template (Automatisch) |

## 4.2 Security Options

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 4200 | Die Verbindung von Benutzer denen die Login-Zeit beschränkt wurde soll nach Ablauf der entsprechenden Zeitgrenze unterbrochen werden. | Microsoft network server: Disconnect clients when logon hours expire<br>Enabled | 💣 | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 4201 | Anonymen Benutzern wird eine SID/Benutzernamen Umsetzung verweigert. | Network access: Allow anonymous SID/Name translation<br>Not defined<br><br>Falls diese Funktion abgeschaltet wird, wird die Funktion von RAS, SQL und Exchange Servern auf NT4.0 eingeschränkt! | 💣💣 | Security Template (Automatisch) |
| 4202 | Die Verbindung von Benutzer denen die Login-Zeit beschränkt wurde soll nach Ablauf der entsprechenden Zeitgrenze unterbrochen werden.<br>DDP: Enabled | Network security: Force logoff when logon hours expire<br>Enabled | 💣 | Security Template (Automatisch) |

## 4.3 Zusätzliche Domain Default Policies

| Nr. | Sicherheitseinstellung | Bemerkung |
|---|---|---|
| 4300 | Kerberos Policy: Enforce user logon restrictions<br>Enabled | Default Domain Policy |
| 4301 | Kerberos Policy: Maximum lifetime for service ticket<br>600 minutes | Default Domain Policy |
| 4302 | Kerberos Policy: Meximum lifetime for user ticket<br>10 hours | Default Domain Policy |
| 4303 | Kerberos Policy: Maximum lifetime for user ticket renewal<br>7 days | Default Domain Policy |
| 4304 | Kerberos Policy: Maximum tolerance for computer clock synchronization<br>5 minutes | Default Domain Policy |

| Nr. | Sicherheitseinstellung | Bemerkung |
|---|---|---|
| 4305 | Public Key Policies/Autoenrollment Settings: Enroll certificates automatically<br>Enabled | Default Domain Policy |
| 4306 | Public Key Policies/Autoenrollment Settings: Renew expired certificates, update pending certificates, and remove revoked certificates<br>Disabled | Default Domain Policy |
| 4307 | Public Key Policies/Autoenrollment Settings: Update certificates that use certificate templates<br>Disabled | Default Domain Policy |
| 4308 | Public Key Policies/Encrypting File System: Allow users to encrypt files using Encrypting File System (EFS)<br>Enabled | Default Domain Policy |
| 4309 | Public Key Policies/Encrypting File System/Certificates<br>Certificate of administrator in order to recovery deleted files | Default Domain Policy |
| 4310 | Public Key Policies/Trusted Root Certification Authorities: Allow users to select new root certification authorities (CAs) to trust<br>Enabled | Default Domain Policy |
| 4311 | Public Key Policies/Trusted Root Certification Authorities: Client computers can trust the following certificate stores<br>Third-Party Root Certification Authorities and Enterprise Root Certification Authorities | Default Domain Policy |
| 4312 | Public Key Policies/Trusted Root Certification Authorities: To perform certificate-based authentication of users and computers, CAs must meet the following criteria<br>Registered in Active Directory only | Default Domain Policy |

# 5 Hardening Member Server

| Wirkungskreis | Anwendung | Compass Template Name |
|---|---|---|
| Dieses Kapitel beschreibt die Sicherheitseinstellungen allen Windows 2003 Server, die als Domänenmitglieder konfiguriert sind. | Die entsprechende INF-Datei wird auf die entsprechende OU angewendet (Memberserver). Siehe Kapitel 7.1. | Intranet_Baseline_Security_MemberServer_CSNC_V1.3.inf |

Manuelle Eingriffe, die nicht via den Group Policies gemacht werden können, müssen auf jedem System einzeln getätigt werden!

## 5.1 Installation

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5100 | Keine Standard-Verzeichnisse wählen | Z.b c:\win2k3 und c:\win2k3\ads | 💣 | Manueller Eingriff |
| 5101 | NTFS für alle Dateisysteme einsetzen | Damit Berechtigungen vergeben können, müssen alle Partitionen mit NTFS formatiert werden. Bestehende FAT Partitionen können mittels `convert` konvertiert werden. | 💣💣 | Manueller Eingriff |
| 5102 | Konfiguration der Länder- und Zeiteinstellung | Deutsch (Schweiz) und entsprechende Zeitzone während der Installation auswählen | 💣 | Manueller Eingriff |
| 5103 | Keine Installation von Client-Software (z.B. Outlook, Word, Excel…) auf dem Server | Auf dem Server sollen keine Officearbeiten erledigt werden. Auch das Surfen im Internet soll weit möglichst eingegrenzt werden. | 💣💣 | Manueller Eingriff |
| 5104 | Aufteilung der Programme und Daten auf separate Partitionen | Die Daten (z.B Webroot bei einem IIS) sollten auf eine separate Partition verschoben werden. | 💣💣 | Manueller Eingriff |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5105 | Entfernen von unnötigen Programmen | Entfernen von:<br>• Aktualisierung von Stammzertifikaten<br>• MSN Explorer<br>• Netzwerkdienste<br>• Outlook Express<br>• Windows Messenger<br><br>Danach sind nur noch folgende Komponenten aktiv: Indexdienst, Internet Explorer, Windows Media Player und einige Zubehör- und Dienstprogramme. | 💣💣 | Manuell – Systemsteuerung – Software<br><br>PS: Zusätzliche Komponenten können entfernt werden, werden aber in der Ansicht versteckt. Um das zu Umgehen editiert man die Datei C:\Windows\inf\sysoc.inf und entfernt überall das Wort HIDE. |

## 5.2 System Configuration

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5200 | Installation des aktuellsten Service Packs | Siehe http://www.microsoft.com/technet/security/tpsrvpck.asp und http://www.microsoft.com/technet/security/current.asp | 💣💣💣 | Manueller Eingriff |
| 5201 | Konfiguration des automatischen Updates für betriebssystembasierte Hoffixes | Benutzung von SUS. Siehe Kapitel 7.5.2 | 💣💣💣 | Manueller Eingriff |
| 5202 | Konfiguration der domänenweiten Zeitsynchronisation | Siehe Kapitel 7.1 | 💣💣 | Manueller Eingriff |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5203 | Einschalten des Remote Desktop Zugriffes | Rechts Klick auf „My Computer“ und den Tab Remote auswählen. Danach „Allow users to connect remotely tho this computer“ auswählen. Unter “Select Remote Users” alle unerwünschten Accounts entfernen. | - | Manueller Eingriff |
| 5204 | Installation und Konfiguration eines Virenscanners | Installation eines Virenscanners der das neue API z.b Norton 8.1) von Windows 2003 benutzt. Konfiguration von regelmässigen Updates (min. 1 mal täglich) | 💣💣💣 | Manueller Eingriff |
| 5205 | Setzen eines starken Passworts für den lokalen Administrator.<br><br>Vorzugsmässig sollte nicht auf allen Servern das selbe Passwort für den lokalen Administrator verwendet werden. | Auf jeder Maschine soll ein anderes Passwort für den lokalen Administrator gewählt werden. Folgende Richtlinien sollen dabei eingehalten werden:<br>• Der Username oder Teile davon sind nicht erlaubt<br>• Kennwort Minimumlänge 6 Zeichen<br>• Drei von den folgenden Zeichenkategorien müssen im Kennwort vorhanden sein: (A-Z, a-z, 0-9, Sonderzeichen) | 💣💣💣 | Manueller Eingriff |

## 5.3 Auditing

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5300 | Anmeldeereignisse überwachen<br>DDCP: Sucess, Failure | Audit account logon events<br>Success, Failure | 💣💣 | Security Template (Automatisch) |
| 5301 | Kontenverwaltung überwachen<br>DDCP: No auditing | Audit account management<br>Success, Failure | 💣💣 | Security Template (Automatisch) |
| 5302 | Active Directory-Zugriff überwachen<br>DDCP: No auditing | Audit directory service access<br>Success, Failure | 💣💣 | Security Template (Automatisch) |
| 5303 | Anmeldeversuche überwachen<br>DDCP: Success | Audit logon events<br>Success, Failure | 💣💣 | Security Template (Automatisch) |
| 5304 | Objektzugriffsversuche überwachen<br>Das Einschaltet dieser Option löst noch keine Logeinträge aus. Eine separate Funktion auf den entsprechenden Objekten (z.B. Dateien, Verzeichnisse) muss erst noch eingeschaltet werden.<br>DDCP: No auditing | Audit object access<br>Success, Failure | 💣💣 | Security Template (Automatisch) |
| 5305 | Richtlinienänderungen überwachen<br>DDCP: No auditing | Audit policy change<br>Success | 💣💣 | Security Template (Automatisch) |
| 5306 | Rechteverwendung überwachen<br>DDCP: No auditing | Audit privilege use<br>No auditing | 💣💣 | Security Template (Automatisch) |
| 5307 | Prozessverfolgung überwachen<br>DDCP: No auditing | Audit process tracking<br>No auditing | 💣💣 | Security Template (Automatisch) |
| 5308 | Systemereignisse überwachen<br>DDCP: No auditing | Audit system events<br>Success | 💣💣 | Security Template (Automatisch) |

## 5.4 User Rights Assignments

Es gilt hier zu beachten, dass viele Einstellungen in diesem Bereich von Software wie Management Tools oder Server Applikationen (z.B. SQL, Exchange...) erweitert werden. Diese Einstellungen werden aussschliesslich auf der lokalen Maschine getätigt. Sind jedoch die gleichen Einstellungen per Group Policies definiert, werden die Modifikationen (durchgeführt durch die Installationsroutinen der Applikationen) überschrieben und sind nicht mehr gültig. Darum sind nur wenige Einstellungen per Group Policy definiert. Es wird auch dringenst empfohlen, nach der Installation des „neuen" Servers resp. Applikation die allefalls lokal getätigten Einstellungen zu prüfen und mit der Group Policy zu vergleichen.

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5400 | Auf diesen Computer vom Netzwerk aus zugreifen<br>DDCP: Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS, Everyone, Pre-Windows 2000 Compatible Access | Access this computer from the network<br>Not Defined | 💣💣 | Security Template (Automatisch) |
| 5401 | Einsetzen als Teil des Betriebssystems<br>DDCP: Nobody | Act as part of the operating system<br>Not Defined | 💣💣 | Security Template (Automatisch) |
| 5402 | Hinzufügen von Arbeitsstationen zur Domäne<br>DDCP: Authenticated Users | Add workstations to domain<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5403 | Anpassen von Speicherkontingenten für einen Prozess<br>DDCP: Administrators, LOCAL SERVICE; NETWORK SERVICE | Adjust memory quotas for a process<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5404 | Lokal anmelden<br>DDCP: Account Operators, Administrators, Backup Operators, Print Operators, Server Operators | Allow log on locally<br>Not defined | 💣💣 | Security Template (Automatisch)<br>→ Entfernen Sie bei den lokalen Einstellungen die Gruppe „Benutzer" resp. „Users" vom „Allow log on locally"-Recht. |
| 5405 | Anmeldung über Terminaldienste zulassen<br>DDCP: Not defined | Allow log on through Terminal Services<br>Administrators, Remote Desktop User | 💣💣 | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5406 | Sichern von Dateien und Verzeichnissen<br>DDCP: Administrators, Backup Operators, Server Operators | Back up files and directories<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5407 | Auslassen der durchsuchenden Überprüfung<br>DDCP: Administrators, Authenticated Users, Everyone, Pre-Windows 2000 Compatible Access | Bypass traverse checking<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5408 | Ändern der Systemzeit<br>DDCP: Administrators, Server Operators | Change the system time<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5409 | Erstellen einer Auslagerungsdatei<br>DDCP: Administators | Create a pagefile<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5410 | Erstellen eines Tokenobjekts<br>DDCP: Nobody | Create a token object<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5411 | Erstellen von globalen Objekten<br>DDCP: Administrators, SERVICE | Create global objects<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5412 | Erstellen von dauerhaft freigegebenen Objekten<br>DDCP: Nobody | Create permanent shared objects<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5413 | Debuggen von Programmen<br>DDCP: Administrators | Debug programs<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5414 | Zugriff vom Netzwerk auf diesen Computer verweigern<br>DDCP: Nobody | Deny access to this computer from the network<br>ANONYMOUS LOGON<br><br>Wird die Gruppe Guests hier eingetragen, funktionieren sämtliche Webserver in der Domäne nicht mehr, da der IUSR-Benutzer in der Gruppe Guest Mitglied ist. | 💣💣 | Security Template (Automatisch) |
| 5415 | Anmeldung als Batchauftrag verweigern<br>DDCP: Nobody | Deny log on as a batch job<br>Guests | 💣💣 | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5416 | Anmeldung als Dienst verweigern<br>DDCP: Nobody | Deny log on as a service<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5417 | Lokale Anmeldung verweigern<br>DDCP: Nobody | Deny log on locally<br>Not defined | 💣 | Security Template (Automatisch) |
| 5418 | Anmeldung über Terminaldienste verweigern<br>DDCP: Not Defined | Deny log on through Terminal Services<br>Built-in Administrator, Guests, Guest, Support_388946a0, all NON-Operating System service accounts (e.g. Exchange, SQL…) | 💣💣 | Manueller Eingriff |
| 5419 | Ermöglichen, dass Computer- und Benutzerkonten für Delegierungszwecke vertraut wird<br>DDCP: Administrators | Enable computer and user accounts to be trusted for delegation<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5420 | Erzwingen des Herunterfahrens von einem Remotesystem aus<br>DDCP: Administrators, Server Operators | Force shutdown from a remote system<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5421 | Generieren von Sicherheitsüberwachungen<br>DDCP: LOCAL SERVICE, NETWORK SERVICE | Generate security audits<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5422 | Starten von Programmen unter einem anderen Benutzer (runas)<br>Achtung: Diese Privileg dürfen nur Administratoren besitzen!<br>DDCP: Administators, SERVICE | Impersonate a client after authentication<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5423 | Anheben der Zeitplanungspriorität<br>DDCP: Administrators | Increase scheduling priority<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5424 | Laden und Entfernen von Gerätetreibern<br>DDCP: Administrators | Load and unload device drivers<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5425 | Sperren von Seiten im Speicher<br>DDCP: Nobody | Lock pages in memory<br>Not Defined | 💣 | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5426 | Anmelden als Stapelverarbeitungsauftrag<br>DDCP: Nobody | Log on as a batch job<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5427 | Als Dienst anmelden<br>DDCP: Nobody | Log on as a service<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5428 | Verwalten von Überwachungs- und Sicherheitsprotokollen<br>DDCP: Administrators | Manage auditing and security log<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5429 | Verändern der Firmwareumgebungsvariablen<br>DDCP: Administrators | Modify firmware environment values<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5430 | Durchführen von Volumewartungsaufgaben<br>DDCP: Not defined | Perform volume maintenance tasks<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5431 | Erstellen eines Profils für einen Einzelprozess<br>DDCP: Administrators | Profile single process<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5432 | Erstellen eines Profils der Systemleistung<br>DDCP: Administrators | Profile system performance<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5433 | Entfernen des Computers von der Dockingstation<br>DDCP: Administrators | Remove computer from docking station<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5434 | Ersetzen eines Tokens auf Prozessebene<br>DDCP: LOCAL SERVICE, NETWORK SERVICE | Replace a process level token<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5435 | Wiederherstellen von Dateien und Verzeichnissen<br>DDCP: Administrators, Backup Operators, Server Operators | Restore files and directories<br>Administrators | 💣 | Security Template (Automatisch) |
| 5436 | Herunterfahren des Systems<br>DDCP: Account Operators, Administrators, Backup Operators, Print Operators, Server Operators | Shut down the system<br>Not Defined | 💣 | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5437 | Synchronisieren von Verzeichnisdienstdaten<br>DDCP: Nobody | Synchronize directory service data<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5438 | Übernehmen des Besitzes von Dateien und Objekten<br>DDCP: Administrators | Take ownership of files or other objects<br>Not Defined | 💣 | Security Template (Automatisch) |

## 5.5 Security Options

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5500 | Konten: Administratorkontostatus | Accounts: Administrator account status<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5501 | Konten: Gastkontenstatus | Accounts: Guest account status<br>Disabled | 💣💣💣 | Security Template (Automatisch) |
| 5502 | Konten: Lokale Kontenverwendung mit leeren Kennwörtern auf Konsolenanmeldung beschränken | Accounts: Limit local account use of blank passwords to console logon only<br>Enabled | 💣💣💣 | Security Template (Automatisch) |
| 5503 | Konten: Administrator umbenennen | Accounts: Rename administrator account<br>Lroot (Local Root) | 💣 | Security Template (Automatisch) |
| 5504 | Konten: Gastkonto umbenennen | Accounts: Rename guest account<br>Not Defined<br>→ Sollte ohnehin disabled sein. | - | Security Template (Automatisch) |
| 5505 | Überwachung: Zugriff auf globale Systemobjekte prüfen | Audit: Audit the access of global system objects<br>Disabled | - | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5506 | Überwachung: Die Verwendung des Sicherungs- und Wiederherstellungsrechts überprüfen | Audit: Audit the use of Backup and Restore privilege<br>Disabled | - | Security Template (Automatisch) |
| 5507 | Überwachung: System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können | Audit: Shut down system immediately if unable to log security audits<br>Disabled | - | Security Template (Automatisch) |
| 5508 | Geräte: Entfernen ohne vorherige Anmeldung erlauben | Devices: Allow undock without having to log on<br>Disabled<br>→ Server sind vermutlich keine Notebooks ;) | - | Security Template (Automatisch) |
| 5509 | Geräte: Formatieren und Auswerfen von Wechselmedien zulassen | Devices: Allowed to format and eject removable media<br>Administrators | 💣 | Security Template (Automatisch) |
| 5510 | Geräte: Anwendern das Installieren von Druckertreibern nicht erlauben | Devices: Prevent users from installing printer drivers<br>Enabled<br>→ Auf Servern muss ein Anwender keinen Drucker installieren können | 💣 | Security Template (Automatisch) |
| 5511 | Geräte: Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken | Devices: Restrict CD-ROM access to locally logged-on user only<br>Enabled | 💣 | Security Template (Automatisch) |
| 5512 | Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken | Devices: Restrict floppy access to locally logged-on user only<br>Enabled | 💣 | Security Template (Automatisch) |
| 5513 | Geräte: Verhalten bei der Installation von nichtsignierten Treibern | Devices: Unsigned driver installation behavior<br>Warn but allow installation | 💣 | Security Template (Automatisch) |
| 5514 | Domänencontroller: Serveroperatoren das Einrichten von geplanten Tasks erlauben | Domain controller: Allow server operators to schedule tasks<br>Disabled<br>→ nur der AT-Befehl ist davon betroffen | 💣💣 | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5515 | Domänencontroller: Signaturanforderungen für LDAP-Server<br><br>DDCP: None | Domain controller: LDAP server signing requirements<br>Not Defined<br>→ LDAP Server laufen nur auf Domänen Controller | - | Security Template (Automatisch) |
| 5516 | Domänencontroller: Änderungen von Computerkontenkennwörtern verweigern | Domain controller: Refuse machine account password changes<br>Disabled<br>→ Nur auf Domain Controllern relevant! | - | Security Template (Automatisch) |
| 5517 | Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)<br><br>DDCP: Enabled | Domain member: Digitally encrypt or sign secure channel data (always)<br>Disabled<br>→ Dies kann nur eingeschaltet werden, wenn min. NT4 SP6a eingesetzt wird. | 💣 | Security Template (Automatisch) |
| 5518 | Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln (wenn möglich) | Domain member: Digitally encrypt secure channel data (when possible)<br>Enabled | 💣 | Security Template (Automatisch) |
| 5519 | Domänenmitglied: Daten des sicheren Kanals digital signieren (wenn möglich) | Domain member: Digitally sign secure channel data (when possible)<br>Enabled | 💣 | Security Template (Automatisch) |
| 5520 | Domänenmitglied: Änderungen von Computerkontenkennwörtern deaktivieren | Domain member: Disable machine account password changes<br>Disabled | 💣💣 | Security Template (Automatisch) |
| 5521 | Domänenmitglied: Maximalalter von Computerkontenkennwörtern | Domain member: Maximum machine account password age<br>30 days | 💣💣 | Security Template (Automatisch) |
| 5522 | Domänenmitglied: Starker Sitzungsschlüssel erforderlich (Windows 2000 oder höher) | Domain member: Require strong (Windows 2000 or later) session key<br>Enabled | 💣💣 | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5523 | Änderung der Beschreibung des originalen Administrators | Gesamte Beschreibung löschen oder so anpassen, dass dieser nicht erkannt wird. | 💣 | Manueller Eingriff (Local Users and Groups) |
| 5524 | Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen | Interactive logon: Do not display last user name<br>Enabled | 💣 | Security Template (Automatisch) |
| 5525 | Interaktive Anmeldung: Kein STRG+ALT+ENTF erforderlich | Interactive logon: Do not require CTRL+ALT+DEL<br>Disabled | 💣 | Security Template (Automatisch) |
| 5526 | Interaktive Anmeldung: Nachricht für Benutzer, die sich anmelden wollen | Interactive logon: Message text for users attempting to log on<br>Dieser Computer, sowie das gesamte Netzwerk eigeschlossen allen Daten sind Firmeneigentum und gesetzlich geschützt. Der Zugriff ist ausschliesslich berechtigten Personen vorbehalten. Die Benutzung dieses Computers sowie dem Netzwerk wird überwacht und protokolliert. | 💣 | Security Template (Automatisch) |
| 5527 | Interaktive Anmeldung: Nachrichtentitel für Benutzer, die sich anmelden wollen | Interactive logon: Message title for users attempting to log on<br>WARNUNG!!! | 💣 | Security Template (Automatisch) |
| 5528 | Interaktive Anmeldung: Anzahl zwischenzuspeichernder vorheriger Anmeldungen (für den Fall, dass der Domänencontroller nicht verfügbar ist) | Interactive logon: Number of previous logons to cache (in case domain controller is not available)<br>0 logons | 💣💣 | Security Template (Automatisch) |
| 5529 | Interaktive Anmeldung: Anwender vor Ablauf des Kennworts zum Ändern des Kennworts auffordern | Interactive logon: Prompt user to change password before expiration<br>10 days | 💣 | Security Template (Automatisch) |
| 5530 | Interaktive Anmeldung: Domänencontrollerauthentifizierung zum Aufheben der Sperrung der Arbeitsstation erforderlich | Interactive logon: Require Domain Controller authentication to unlock workstation<br>Enabled | 💣💣 | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5531 | Interaktive Anmeldung: Zur Anmeldung wird eine SmartCard benötigt | Interactive logon: Require smart card<br>Not defined | - | Security Template (Automatisch) |
| 5532 | Interaktive Anmeldung: Verhalten beim Entfernen von Smartcards | Interactive logon: Smart card removal behavior<br>Lock Workstation | 💣 | Security Template (Automatisch) |
| 5533 | Microsoft-Netzwerk (Client): Kommunikation digital signieren (immer) | Microsoft network client: Digitally sign communications (always)<br>Disabled | 💣💣 | Security Template (Automatisch) |
| 5534 | Microsoft-Netzwerk (Client): Kommunikation digital signieren (wenn Server zustimmt) | Microsoft network client: Digitally sign communications (if server agrees)<br>Enabled | 💣💣 | Security Template (Automatisch) |
| 5535 | Microsoft-Netzwerk (Client): Unverschlüsseltes Kennwort an SMB-Server von Drittanbietern senden | Microsoft network client: Send unencrypted password to third-party SMB servers<br>Disabled | 💣💣💣 | Security Template (Automatisch) |
| 5536 | Microsoft-Netzwerk (Server): Leerlaufzeitspanne bis zum Anhalten der Sitzung | Microsoft network server: Amount of idle time required before suspending session<br>15 minutes | 💣 | Security Template (Automatisch) |
| 5537 | Microsoft-Netzwerk (Server): Kommunikation digital signieren (immer)<br>DDCP: Enabled | Microsoft network server: Digitally sign communications (always)<br>Disabled | 💣💣 | Security Template (Automatisch) |
| 5538 | Microsoft-Netzwerk (Server): Kommunikation digital signieren (wenn Client zustimmt)<br>DDCP: Enabled | Microsoft network server: Digitally sign communications (if client agrees)<br>Enabled | 💣💣 | Security Template (Automatisch) |
| 5539 | Microsoft-Netzwerk (Server): Clientverbindungen aufheben, wenn die Anmeldezeit überschritten wird | Microsoft network server: Disconnect clients when logon hours expire<br>Enabled | 💣 | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5540 | Netzwerkzugriff: Anonyme SID-/Namensübersetzung zulassen | Network access: Allow anonymous SID/Name translation<br>Not definded | 💣💣 | Security Template (Automatisch) |
| 5541 | Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten nicht erlauben | Network access: Do not allow anonymous enumeration of SAM accounts<br>Enabled | 💣💣 | Security Template (Automatisch) |
| 5542 | Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten und Freigaben nicht erlauben | Network access: Do not allow anonymous enumeration of SAM accounts and shares<br>Enabled | 💣💣 | Security Template (Automatisch) |
| 5543 | Netzwerkzugriff: Speicherung von Anmeldeinformationen oder .NET-Passports für die Netzwerkauthentifikation nicht erlauben | Network access: Do not allow storage of credentials or .NET Passports for network authentication<br>Enabled | 💣 | Security Template (Automatisch) |
| 5544 | Netzwerkzugriff: Die Verwendung von 'Jeder'-Berechtigungen für anonyme Benutzer ermöglichen | Network access: Let Everyone permissions apply to anonymous users<br>Disabled<br>→ Domänen-Trusts mit NT4 Domänen können so nicht mehr eingegangen werden | 💣💣 | Security Template (Automatisch) |
| 5545 | Netzwerkzugriff: Named Pipes, auf die anonym zugegriffen werden kann | Network access: Named Pipes that can be accessed anonymously<br>None | 💣💣 | Security Template (Automatisch) |
| 5546 | Netzwerkzugriff: Registrierungspfade, auf die von anderen Computern aus zugegriffen werden kann | Network access: Remotely accessible registry paths<br>System\CurrentControlSet\Control\ProductOptions<br>System\CurrentControlSet\Control\Server Applications<br>Software\Microsoft\Windows NT\CurrentVersion | - | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5547 | Netzwerkzugriff: Registrierungsunterpfade, auf die von anderen Computern aus zugegriffen werden kann | Network access: Remotely accessible registry paths and sub-paths<br>Software\Microsoft\Windows NT\CurrentVersion\Print,Software\Microsoft\Windows NT\CurrentVersion\Windows<br>System\CurrentControlSet\Control\Print\Printers<br>System\CurrentControlSet\Services\Eventlog<br>Software\Microsoft\OLAP Server<br>System\CurrentControlSet\Control\ContentIndex<br>System\CurrentControlSet\Control\Terminal Server<br>System\CurrentControlSet\Control\Terminal Server\UserConfig<br>System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration<br>Software\Microsoft\Windows NT\CurrentVersion\Perflib<br>System\CurrentControlSet\Services\SysmonLog | - | Security Template (Automatisch) |
| 5548 | Netzwerkzugriff: Verbieten von anonymen Verbindungen auf Named Pipes und Freigaben | Network access: Restrict anonymous access to Named Pipes and Shares<br>Enabled | 💣💣 | Security Template (Automatisch) |
| 5549 | Netzwerkzugriff: Freigaben, auf die anonym zugegriffen werden kann | Network access: Shares that can be accessed anonymously<br>None | 💣💣💣 | Security Template (Automatisch) |
| 5550 | Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten | Network access: Sharing and security model for local accounts<br>Classic - local users authenticate as themselves | 💣💣💣 | Security Template (Automatisch) |
| 5551 | Netzwerksicherheit: Keine LAN Manager-Hashwerte für nächste Kennwortänderung speichern | Network security: Do not store LAN Manager hash value on next password change<br>Enabled<br>→ Alle Passwörter müssen neu vergeben werden. Diese Einstellung gilt nur für neue Passwörter! | 💣💣 | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5552 | Netzwerksicherheit: Abmeldung nach Ablauf der Anmeldezeit erzwingen | Network security: Force logoff when logon hours expire<br>Not Defined<br>→ Auf Domänenebene definiert | - | Security Template (Automatisch) |
| 5553 | Netzwerksicherheit: LAN Manager-Authentifizierungsebene<br><br>DDCP: Send NTLM response only | Network security: LAN Manager authentication level<br>Send NTLMv2 response only\refuse LM & NTLM<br>→ Achtung beim Einsatz von Routing and Remote Access Server. Da muss diese Einstellung auf …\refuse LM zurückgestuft werden. | 💣💣💣 | Security Template (Automatisch) |
| 5554 | Netzwerksicherheit: Signaturanforderungen für LDAP-Clients | Network security: LDAP client signing requirements<br>Negotiate signing | 💣 | Security Template (Automatisch) |
| 5555 | Netzwerksicherheit: Minimale Sitzungssicherheit für NTLM-SSP-basierte Clients (einschließlich sicherer RPC-Clients) | Network security: Minimum session security for NTLM SSP based (including secure RPC) clients<br>No Minimum | 💣💣 | Security Template (Automatisch) |
| 5556 | Netzwerksicherheit: Minimale Sitzungssicherheit für NTLM-SSP-basierte Server (einschließlich sicherer RPC-Server) | Network security: Minimum session security for NTLM SSP based (including secure RPC) servers<br>No Minimum | 💣💣 | Security Template (Automatisch) |
| 5557 | Wiederherstellungskonsole: Automatische administrative Anmeldungen zulassen | Recovery console: Allow automatic administrative logon<br>Disabled | 💣💣 | Security Template (Automatisch) |
| 5558 | Wiederherstellungskonsole: Kopieren von Disketten und Zugriff auf alle Laufwerke und alle Ordner zulassen | Recovery console: Allow floppy copy and access to all drives and all folders<br>Enabled | - | Security Template (Automatisch) |
| 5559 | Herunterfahren: Herunterfahren des Systems ohne Anmeldung zulassen | Shutdown: Allow system to be shut down without having to log on<br>Disabled | 💣💣 | Security Template (Automatisch) |
| 5560 | Herunterfahren: Auslagerungsdatei des virtuellen Arbeitspeichers löschen | Shutdown: Clear virtual memory pagefile<br>Disabled | - | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5561 | Systemkryptografie: Benutzerspezifische Schlüssel (z.B. SSL Clientcertifikate) sollen mit einen starken Schlüssel geschützt werden | System cryptography: Force strong key protection for user keys stored on the computer<br>User is prompted when the key is first used | 💣 | Security Template (Automatisch) |
| 5562 | Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden | System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing<br>Disabled | 💣 | Security Template (Automatisch) |
| 5563 | Systemobjekte: Standardbesitzer für Objekte, die von Mitgliedern der Administratorengruppe erstellt werden | System objects: Default owner for objects created by members of the Administrators group<br>Object creator | 💣💣 | Security Template (Automatisch) |
| 5564 | Systemobjekte: Groß-/Kleinschreibung für Nicht-Windows-Subsysteme ignorieren | System objects: Require case insensitivity for non-Windows subsystems<br>Enabled<br>→ Weiter oben wurden alle Subsysteme entfernt! | - | Security Template (Automatisch) |
| 5565 | Systemobjekte: Standardberechtigungen interner Systemobjekte (z. B. symbolischer Verknüpfungen) verstärken | System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)<br>Enabled | 💣 | Security Template (Automatisch) |
| 5566 | Systemeinstellungen: Optionale Subsysteme | System settings: Optional subsystems<br>None | 💣 | Security Template (Automatisch) |
| 5567 | Systemeinstellungen: Benutzen von Zertifikatregeln bei ausführbaren Dateien bei der Benutzung von Software Richtlinien | System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies<br>Not Defined<br>→ Die Einführung von Software Restriction Policies bedarf einer guten Planung. Zudem muss eine CA aufgebaut werden. | - | Security Template (Automatisch) |

## 5.6 Event Log

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5600 | Maximale Protokollgrösse (Anwenung) | Maximum application log size<br>16000 kilobytes | 💣💣 | Security Template (Automatisch) |
| 5601 | Maximale Protokollgrösse (Sicherheit) | Maximum security log size<br>96000 kilobytes | 💣💣 | Security Template (Automatisch) |
| 5602 | Maximale Protokollgrösse (System) | Maximum system log size<br>16000 kilobytes | 💣💣 | Security Template (Automatisch) |
| 5603 | Sperren des Zugriffs auf die Anwendungsprotokolierung für Gäste | Prevent local guests group from accessing application log<br>Enabled | 💣💣 | Security Template (Automatisch) |
| 5604 | Sperren des Zugriffs auf die Sicherheitsprotokolierung für Gäste | Prevent local guests group from accessing security log<br>Enabled | 💣💣 | Security Template (Automatisch) |
| 5605 | Sperren des Zugriffs auf die Systemprotokolierung für Gäste | Prevent local guests group from accessing system log<br>Enabled | 💣💣 | Security Template (Automatisch) |
| 5606 | Ergreignisse überschreiben, die älter als x-Tage sind (Anwendungsprotokoll) | Retain application log<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5607 | Ergreignisse überschreiben, die älter als x-Tage sind (Sicherheitsprotokoll) | Retain security log<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5608 | Ergreignisse überschreiben, die älter als x-Tage sind (Systemprotokoll) | Retain system log<br>Not Defined | 💣 | Security Template (Automatisch) |
| 5609 | Ereignisse nach Bedarf überschreiben (Anwendungsprotokoll) | Retention method for application log<br>As needed | 💣💣 | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5610 | Ereignisse nach Bedarf überschreiben (Sicherheitsprotokoll) | Retention method for security log<br>As needed | 💣💣 | Security Template (Automatisch) |
| 5611 | Ereignisse nach Bedarf überschreiben (Systemprotokoll) | Retention method for system log<br>As needed | 💣💣 | Security Template (Automatisch) |

## 5.7 System Services

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5700 | Nachrichtendienst<br>Überträgt NET SEND- und Warndienstnachrichten zwischen Clients und Servern. Dieser Dienst ist nicht mit Windows Messenger verwandt. Der Warndienst überträgt keine Nachrichten, falls dieser Dienst beendet wird. Falls dieser Dienst deaktiviert wird, können die Dienste, die von diesem Dienst ausschließlich abhängig sind, nicht mehr gestartet werden. | Alerter<br>Enabled<br><br>Wird für das versenden von Warnachrichten benötigt (z.B. USV) | 💣 | Security Template (Automatisch) |
| 5701 | Gatewaydienst auf Anwendungsebene<br>Bietet Unterstützung für Protokoll-Plug-Ins von Drittanbietern für die gemeinsame Nutzung der Internetverbindung und den Internetverbindungsdfirewall. | Application Layer Gateway Service<br>Disabled<br>→ Diese Funktionalität wird auf einem Server nicht benötigt! | 💣 | Security Template (Automatisch) |
| 5702 | Anwendungsverwaltung<br>Bietet Softwareinstallationsdienste wie Zuweisung, Veröffentlichung, und Deinstallation. | Application Management<br>Disabled<br>→ Wird benötigt wenn über Group Policy Programme installiert werdem | 💣 | Security Template (Automatisch) |
| 5703 | Provides support for out-of-process session states for ASP.NET. If this service is stopped, out-of-process requests will not be processed. | ASP .NET State Service<br>Disabled | 💣 | Security Template (Automatisch) |
| 5704 | Automatische Updates<br>Aktiviert den Download und die Installation für wichtige Updates von Windows Update. Das Betriebssystem kann manuell über die Windows Update-Website aktualisiert werden, falls der Dienst deaktiviert wird. | Automatic Updates<br>Disabled<br><br>Wird im Zusammenhang mit SUS bennötigt. Siehe Kapitel 0 | 💣💣💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5705 | Intelligenter Hintergrundübertragungsdienst<br>Verwendet sich in Leerlauf befindende Netzwerkbandbreite für die Datenübertragung. | Background Intelligent Transfer Service<br>Manual | 💣 | Security Template (Automatisch) |
| 5706 | Zertifikat Service<br>Dient zum Austellen und Managem von Digitalen Zertifikaten. | Certifcate Service<br>Disabled | 💣 | Security Template (Automatisch) |
| 5707 | Client Service für Novell Netware<br>Für den Zugriff auf Novell Netzwerkressourcen wie Dateien. | Client Service for Netware<br>Disabled | 💣 | Security Template (Automatisch) |
| 5708 | Ablagemappe<br>Ermöglicht der Ablagemappe, Informationen zu speichern und mit Remotecomputern auszutauschen. Wenn dieser Dienst beendet wird, wird die Ablagemappe keine Informationen mehr mit Remotecomputern austauschen können. Wenn dieser Dienst deaktiviert wird, werden alle von diesem Dienst explizit abhängigen Dienste nicht gestartet werden können. | ClipBook<br>Disabled | 💣 | Security Template (Automatisch) |
| 5709 | Cluster Service<br>Stellt Hochverfügbarkeit zur Verfügung. | Cluster Service<br>Not defined | 💣 | Security Template (Automatisch) |
| 5710 | COM+-Ereignissystem<br>Unterstützt den Systemereignis-Benachrichtigungsdienst (SENS, System Event Notification Service), der die automatische Verteilung von Ereignissen an abonnierende COM-Komponenten zur Verfügung stellt. Wenn der Dienst beendet ist, wird SENS beendet und ist nicht in der Lage Anmelde- und Abmeldebenachrichtigungen zur Verfügung zu stellen. Wenn der Dienst deaktiviert ist, können abhängige Dienste nicht gestartet werden. | COM+ Event System<br>Manual | 💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5711 | COM+-Systemanwendung<br>Verwaltet die Komponentenkonfiguration und -überwachung von COM+-basierten Komponenten. Nach dem Beenden des Dienstes sind die meisten COM+-basierten Komponenten nicht ordnungsgemäß funktionsfähig. Nach dem Deaktivieren dieses Dienstes werden alle Dienste nicht gestartet, die explizit auf diesem Dienst basieren. | COM+ System Application<br>Disabled | 💣 | Security Template (Automatisch) |
| 5712 | Computerbrowser<br>Führt eine aktuelle Liste der Computer im Netzwerk und gibt diese an als Browser fungierende Computer weiter. Diese Liste wird nicht aktualisiert oder gewartet, falls der Dienst beendet wird. Falls dieser Dienst deaktiviert wird, können die Dienste, die von diesem ausschließlich Dienst abhängig sind, nicht mehr gestartet werden. | Computer Browser<br>Automatic | - | Security Template (Automatisch) |
| 5713 | Kryptografiedienste<br>Stellt drei Verwaltungsdienste bereit: den Katalogdatenbankdienst, der die Signaturen von Windows-Dateien bestätigt | Cryptographc Services<br>Automatic | 💣 | Security Template (Automatisch) |
| 5714 | DHCP-Client<br>Verwaltet die Netzwerkkonfiguration, indem IP-Adressen und DNS-Namen registriert und aktualisiert werden. | DHCP Client<br>Automatic | - | Security Template (Automatisch) |
| 5715 | DHCP-Server<br>Stellt die dynamische Netzwerkkonfiguration zur Verfügung, indem IP-Adressen und DNS-Namen an DHCP-Clients verteilt werden. | DHCP Server<br>Disabled | 💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5716 | Verteiltes Dateisystem<br>DFS managen logische Volumes, die über das Netzwerk verteilt sind. | Distributed File System<br>Disabled | 💣 | Security Template (Automatisch) |
| 5717 | Überwachung verteilter Verknüpfungen (Client)<br>Hält Verknüpfungen für NTFS-Dateien auf einem Computer oder zwischen Computern in einer Netzwerkdomäne aufrecht. | Distributed Link Tracking Client<br>Disabled<br>→ NTFS-Links werden auf dem lokalen Computer nicht mehr gewartet oder verfolgt. | 💣 | Security Template (Automatisch) |
| 5718 | Überwachung verteilter Verknüpfungen (Server) | Distributed Link Tracking Server<br>Disabled<br>→ NTFS-Links werden auf dem lokalen Computer nicht mehr gewartet oder verfolgt. | 💣 | Security Template (Automatisch) |
| 5719 | Distributed Transaction Coordinator<br>Koordiniert Transaktionen, die sich über mindestens zwei Ressourcenverwaltungen wie Datenbanken, Nachrichtenwarteschlangen oder Dateisysteme erstrecken. Wenn der Dienst beendet ist, treten diese Transaktionen nicht auf. Wenn der Dienst deaktiviert ist, können abhängige Dienste nicht gestartet werden. | Distributed Transaction Coordinator<br>Disabled | 💣 | Security Template (Automatisch) |
| 5720 | DNS-Client<br>Wertet DNS-Namen (Domain Name System) für diesen Computer aus und speichert sie zwischen. Falls dieser Dienst beendet wird, kann der Computer keine DNS-Namen auflösen und Active Directory-Domänencontroller ermitteln. Falls dieser Dienst deaktiviert wird, können die Dienste, die von diesem Dienst ausschließlich abhängig sind, nicht mehr gestartet werden. | DNS Client<br>Automatic | - | Security Template (Automatisch) |
| 5721 | DNS Server<br>Stellt ein Dienst zur Namensauflösung zur Verfügung. | DNS Server<br>Disabled | 💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5722 | Fehlerberichterstattungsdienst<br>Ermöglicht die Fehlerberichterstattung für Dienste und Anwendungen, die in nicht standardgemäßen Umgebungen ausgeführt werden. | Error Reporting Service<br>Disabled | 💣💣 | Security Template (Automatisch) |
| 5723 | Ereignisprotokoll<br>Ermöglicht die Ansicht von Ereignisprotokollmeldungen von Windows-basierten Programmen und Komponenten in der Ereignisanzeige. Dieser Dienst kann nicht beendet werden. | Event Log<br>Automatic | 💣💣 | Security Template (Automatisch) |
| 5724 | Fax Dienst<br>Stellt Fax Funktionalität zur Verfügung. | Fax Service<br>Disabled | 💣 | Security Template (Automatisch) |
| 5725 | Datei Replikation<br>Repliziert Dateien über verschiedene Server. | File Replication<br>Disabled<br>→ Wird auf Domain Controller benötigt! | 💣 | Security Template (Automatisch) |
| 5726 | Datei Server für Macintosh<br>Macinthosh Benutzer können auf den Windwos Server zugreifen. | File Server for Macinthosh<br>Disabled | 💣 | Security Template (Automatisch) |
| 5727 | FTP Dienst<br>Stellt das File Transfer Protokoll zur Verfügung. (Teil des IIS). | FTP Publishing Service<br>Disabled | 💣💣 | Security Template (Automatisch) |
| 5728 | Hilfe und Support<br>Aktiviert das Hilfe- und Supportcenter auf diesem Computer. Das Hilfe- und Supportcenter ist nicht verfügbar, wenn dieser Dienst beendet wird. Falls dieser Dienst deaktiviert wird, können die Dienste, die von diesem Dienst ausschließlich abhängig sind, nicht mehr gestartet werden. | Help and Support<br>Disabled | 💣💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5729 | HTTP SSL<br>Ist die SSL Komponente des IIS. | HTTP SSL<br>Disabled | 💣 | Security Template (Automatisch) |
| 5730 | Eingabegerätezugang<br>Ermöglicht einen Standardeingabezugang für Eingabegeräte (HID-Geräte), welcher die Verwendung von vordefinierten Schnelltasten auf Tastaturen, Fernbedienungen und anderen Multimediageräten aktiviert und unterstützt. Wenn dieser Dienst beendet wird, werden die von diesem Dienst gesteuerten Schnelltasten nicht mehr funktionieren. Wenn dieser Dienst deaktiviert wird, werden alle von diesem Dienst explizit abhängigen Dienste nicht gestartet werden können. | Human Interface Device Access<br>Disabled | 💣 | Security Template (Automatisch) |
| 5731 | IAS Jet Datenbank Zugriff<br>Kann benutzt werden um Benutzer via den Radius Server zu authentisieren. | IAS Jet Database Access<br>Disabled<br>→ Nur auf der 64-bit Version verfügbar | 💣 | Security Template (Automatisch) |
| 5732 | IIS Admin Dienst<br>Wird für die Administration des IIS benötigt. | IIS Admin Service<br>Disabled | 💣 | Security Template (Automatisch) |
| 5733 | IMAPI-CD-Brenn-COM-Dienste<br>Verwaltet das Aufnehmen von CDs mit IMAPI (Image Mastering Applications Programming Interface). Auf diesem Computer können keine CDs aufgenommen werden, wenn dieser Dienst angehalten wird. Falls dieser Dienst deaktiviert wird, können die Dienste, die von diesem Dienst ausschließlich abhängig sind, nicht mehr gestartet werden. | IMAPI CD-Burning COM Service<br>Disabled | 💣 | Security Template (Automatisch) |
| 5734 | Indexdienst<br>Indiziert Dateiinhalt und -eigenschaften auf lokalen und Remotecomputer und bietet schnellen Dateizugriff durch eine flexible Abfragesprache. | Indexing Service<br>Disabled | 💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5735 | Infrarot Monitor<br>Infrarot Unterstützung. Geräte im Empfangsbereich werden automatisch erkannt. | Infrared Monitor<br>Disabled | 💣 | Security Template (Automatisch) |
| 5736 | Internet Authentisierungs Dienst<br>Stellt einen Radius (Remote Authentication Dial-In User Service) zur Verfügung. Wird oft in Zusammenhang mit VPN oder Wirelessnetzwerken benutzt. | Internet Authentication Service<br>Disabled | 💣 | Security Template (Automatisch) |
| 5737 | Internetverbindungsfirewall/Gemeinsame Nutzung der Internetverbindung<br>Bietet allen Computern in Privat- und Kleinunternehmensnetzwerken Dienste für die Netzwerkadressübersetzung, Adressierung, Namensauflösung und Eindringsschutz. | Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)<br>Disabled | 💣 | Security Template (Automatisch) |
| 5738 | Intersite Mangement<br>Dieser Service wird von Domain Controllern für die Replizierung zwischen Sites verwendet. | Intersite Management<br>Disabled<br>→ Wird auf Domain Controller benötigt! | 💣 | Security Template (Automatisch) |
| 5739 | IP Version 6 Helper Service<br>IPv6 Protokoll. Kann in existierenden IPv4 Netzen verwendet werden. | IP Version 6 Helper Service<br>Disabled | 💣 | Security Template (Automatisch) |
| 5740 | IPSEC-Dienste<br>Verwaltet IP-Sicherheitsrichtlinien und startet den IKE-Treiber (ISAKMP/Oakley) und den IP-Sicherheitstreiber. | IPSEC Services<br>Automatic | 💣 | Security Template (Automatisch) |
| 5741 | Kerberos Schlüssel Verteilungs Dienst<br>Wird auf DC benötigt. Implementiert einen Authentication und den Ticket Granting Service. | Kerberos Key Distribution Center<br>Disabled<br>→ Wird auf Domain Controller benötigt! | 💣 | Security Template (Automatisch) |
| 5742 | Lizenz Verwaltung<br>Trackt Software Lizenzen von Microsoft Produkten. | License Logging Service<br>Disabled | 💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5743 | Administrativer Dienst für den Verwaltungsdienst für die Verwaltung logischer Datenträger<br>Ist zusammen mit dem Logical Disk Manager für die Einrichtung neuer Festplatten zuständig. Dieser Dienst wird nur zu Konfigurationszwecken ausgeführt und anschließend beendet. | Logical Disk Manager Administrative Service<br>Manual | | Security Template (Automatisch) |
| 5744 | Verwaltungsdienst für die Verwaltung logischer Datenträger<br>Konfiguriert Festplattenlaufwerke und -volumes. Dieser Dienst wird nur zu Konfigurationszwecken ausgeführt und anschließend beendet. | Logical Disk Manager<br>Manual | 💣 | Security Template (Automatisch) |
| 5745 | Message Queuing Down Level Clients | Message Queuing Down Level Clients<br>Disabled | 💣 | Security Template (Automatisch) |
| 5746 | Message Queuing Triggers | Message Queuing Triggers<br>Disabled | 💣 | Security Template (Automatisch) |
| 5747 | Message Queuing | Message Queuing<br>Disabled | 💣 | Security Template (Automatisch) |
| 5748 | Messenger<br>Übermittelt net send und Alerter Nachrichten zwischen Clients und Server. | Messenger<br>Automatic | 💣 | Security Template (Automatisch) |
| 5749 | Microsoft POP3 Service<br>Zusammen mit dem SMTP Server wird ein einfacher Mailserver zur Verfügung gestellt. | Microsoft POP3 Service<br>Disabled | 💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5750 | MS Software Shadow Copy Provider<br>Verwaltet Software-basierte Schattenkopien des Volumeschattenkopie-Dienstes. Software-basierte Schattenkopien können nicht verwaltet werden, wenn dieser Dienst beendet wird. Falls dieser Dienst deaktiviert wird, können die Dienste, die von diesem Dienst ausschließlich abhängig sind, nicht mehr gestartet werden. | Microsoft Software Shadow Copy Provider<br>Manual<br>→ Softwarebasierte Schattenkopien können nicht mehr gemanagt werden! | 💣 | Security Template (Automatisch) |
| 5751 | MSSQL$UUDI<br>Stellt eine Hauptkomponente für Webservices dar. Benutzer können Anfragen bezüglich Daten in der SQL-Datenbank stellen. | MSSQL$UUDI<br>Disabled | 💣💣 | Security Template (Automatisch) |
| 5752 | MSSQLServerADHelper<br>Wird benötigt, wenn Informationen ins Active Directory gespeichtert werden möchten, jedoch der SQL Server nicht unter dem System Konto läuft. | MSSQLServerADHelper<br>Disabled | 💣 | Security Template (Automatisch) |
| 5753 | Anmeldedienst<br>Unterstützt Durchsatzauthentifizierung von Kontoanmeldungsereignissen für Computer in einer Domäne. | Net Logon<br>Automatic | 💣 | Security Template (Automatisch) |
| 5754 | NetMeeting-Remotedesktop-Freigabe<br>Ermöglicht einem autorisierten Benutzer an einem anderen Computer auf diesen Computer mit NetMeeting über ein Firmenintranet zuzugreifen. Wenn dieser Dienst beendet wird, ist die Remotedesktopfreigabe nicht mehr verfügbar. Falls dieser Dienst deaktiviert wird, können die Dienste, die von diesem Dienst ausschließlich abhängig sind, nicht mehr gestartet werden. | NetMeeting Remote Desktop Sharing<br>Disabled | 💣💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5755 | Netzwerkverbindungen<br>Verwaltet Objekte im Ordner 'Netzwerk- und DFÜ-Verbindungen' , in dem sowohl LAN-, als auch WAN-Verbindungen angezeigt werden. | Network Connections<br>Manual | 💣 | Security Template (Automatisch) |
| 5756 | Netzwerk-DDE-Serverdienst<br>Verwaltet DDE-Netzwerkfreigaben (Dynamic Data Exchange=Dynamischer Datenaustausch). Wenn dieser Dienst beendet wird, werden keine DDE-Netzwerkfreigaben mehr zur Verfügung stehen. Wenn dieser Dienst deaktiviert wird, werden alle von diesem Dienst explizit abhängigen Dienste nicht gestartet werden können. | Network DDE DSDM<br>Disabled | 💣 | Security Template (Automatisch) |
| 5757 | Netzwerk-DDE-Dienst<br>Ermöglicht Netzwerktransport und Sicherheit für den dynamischen Datenaustausch (DDE) von Programmen, die auf dem gleichen Computer oder auf verschiedenen Computern ausgeführt werden. Wenn dieser Dienst beendet wird, wird der DDE-Transport und die DDE-Sicherheit nicht mehr zur Verfügung stehen. Wenn dieser Dienst deaktiviert wird, werden alle von diesem Dienst explizit abhängigen Dienste nicht gestartet werden können. | Network DDE<br>Disabled | 💣 | Security Template (Automatisch) |
| 5758 | NLA (Network Location Awareness)<br>Sammelt und speichert Netzwerkkonfigurations- und Standortinformationen und benachrichtigt Anwendungen, wenn diese Informationen sich ändern. | Network Location Awareness (NLA)<br>Manual | 💣 | Security Template (Automatisch) |
| 5759 | NNTP Service<br>Unterstützt die zentrale Speicherung von Nachrichten (News). Ist eine Komponente von IIS. | Network News Transport Protocol (NNTP)<br>Disabled | 💣💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5760 | NT-LM-Sicherheitsdienst<br>Bietet Sicherheit für Remoteprozeduraufrufe (RPC), die andere Transportwege als Named Pipes verwenden. | NT LM Security Support Provider<br>Automatic | - | Security Template (Automatisch) |
| 5761 | Leistungsdatenprotokolle und Warnungen<br>Sammelt basierend auf einem vorkonfigurierten Zeitplan Systemleistungsdaten vom lokalen oder von Remotecomputern und schreibt die Daten in ein Protokoll oder löst eine Warnung aus. Wenn dieser Dienst beendet wird, werden keine Leistungsinformationen mehr gesammelt. Wenn dieser Dienst deaktiviert wird, werden alle von diesem Dienst explizit abhängigen Dienste nicht gestartet werden können. | Performance Logs and Alerts<br>Manual | - | Security Template (Automatisch) |
| 5762 | Plug & Play<br>Ermöglicht dem Computer, Hardwareänderungen zu erkennen und sich ohne oder mit geringer Benutzerinteraktion darauf einzustellen. Beenden oder Deaktivieren dieses Dienstes wird die Systemstabilität beeinträchtigen. | Plug and Play<br>Automatic | - | Security Template (Automatisch) |
| 5763 | Seriennummer der tragbaren Medien<br>Ermittelt die Seriennummer aller tragbaren Musikabspielgeräte, die an den Computer angeschlossen sind. | Portable Media Serial Number Service<br>Disabled |  | Security Template (Automatisch) |
| 5764 | Print Server für Macintosh<br>Stellt einen Printserver für Macintosh Clients zur Verfügung. | Print Server for Macintosh<br>Disabled |  | Security Template (Automatisch) |
| 5765 | Druckwarteschlange<br>Lädt die Dateien in den Arbeitsspeicher, um sie später zu drucken. | Print Spooler<br>Disabled |  | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5766 | Geschützter Speicher<br>Bietet geschützten Speicherplatz für private Daten, wie z. B. private Schlüssel, um Zugriff durch nicht autorisierte Dienste, Prozesse oder Benutzer zu unterbinden. | Protected Storage<br>Automatic | 💣 | Security Template (Automatisch) |
| 5767 | Routing und RAS<br>Bietet Routingdienste in LAN- und WAN-Netzwerkumgebungen. | Remote Access Auto Connection Manager<br>Disabled | 💣 | Security Template (Automatisch) |
| 5768 | RAS-Verbindungsverwaltung<br>Stellt eine Netzwerkverbindung her. | Remote Access Connection Manager<br>Disabled | 💣 | Security Template (Automatisch) |
| 5769 | Remote Administrations Dienst<br>Wird vom Remote Server Manager gestartet und führt dessen Anfragen aus, | Remote Administration Service<br>Manual | - | Security Template (Automatisch) |
| 5770 | Sitzungs-Manager für Remotedesktophilfe<br>Verwaltet und überwacht die Remoteunterstützung. Die Remoteunterstützung wird beim Beenden dieses Dienstes nicht verfügbar sein. Bevor Sie diesen Dienst beenden, schauen Sie sich die Registerkarte "Abhängigkeiten" im Dialog "Eigenschaften" an." | Remote Desktop Help Session Manager<br>Disabled | 💣 | Security Template (Automatisch) |
| 5771 | Remote Installations Service<br>RIS ist ein Installationsdienst, mit welchem Betriebssysteme über das Netzwerk installiert werden können. | Remote Installation<br>Disabled<br>→ Wird allenfalls auf Installationsserver benötigt (RIS) | 💣 | Security Template (Automatisch) |
| 5772 | Remoteprozeduraufruf (RPC)<br>Endpunktzuordnung und andere verschiedene RPC-Dienste. | Remote Procedure Call (RPC) Locator<br>Disabled | 💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5773 | RPC-Locator<br>Verwaltet die Datenbank für den RPC-Namensdienst. | Remote Procedure Call (RPC)<br>Automatic | 💣 | Security Template (Automatisch) |
| 5774 | Remote-Registrierung<br>Ermöglicht Remotebenutzern, Registrierungseinstellungen dieses Computers zu verändern. Wenn dieser Dienst beendet wird, kann die Registrierung nur von lokalen Benutzern dieses Computers verändert werden. Wenn dieser Dienst deaktiviert wird, werden alle von diesem Dienst explizit abhängigen Dienste nicht gestartet werden können. | Remote Registry Service<br>Automatic | 💣 | Security Template (Automatisch) |
| 5775 | Remote Server Manager | Remote Server Manager<br>Disabled | 💣 | Security Template (Automatisch) |
| 5776 | Remote Server Monitor | Remote Server Monitor<br>Disabled | 💣 | Security Template (Automatisch) |
| 5777 | Remote Storage Notification | Remote Storage Notification<br>Disabled | 💣 | Security Template (Automatisch) |
| 5778 | Remote Storage Server<br>Stellt Speicher zur Verfügung indem nicht benötigte Daten auf entfernten Speicher ausgelagert werden. | Remote Storage Server<br>Disabled | 💣 | Security Template (Automatisch) |
| 5779 | Wechselmedien<br>Wird benötigt bei Bandlaufwerden und Jukeboxen. | Removable Storage<br>Disabled<br>→ Wird benötigt, wenn mit ntbackup Sicherheitskopien erstellt werden | 💣 | Security Template (Automatisch) |
| 5780 | Resultant Set of Policy Provider (RSoP)<br>Wird benötigt, wenn die tätsächlich angewendeten Policies ausgelesen werden möchten. | Resultant Set of Policy Provider<br>Disabled | 💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5781 | Verwaltung für automatische RAS-Verbindung<br>Erstellt eine Verbindung zu einem Remotenetzwerk, wenn ein Programm eine Remote-DNS- oder -NetBIOS-Adresse referenziert. | Routing and Remote Access<br>Disabled | 💣 | Security Template (Automatisch) |
| 5782 | SAP Agent<br>Wird im Zusammenhang mit IPX benötigt um freigegebene Resourcen auf dem Netzwerk bekannt zu machen. | SAP Agent<br>Disabled | 💣 | Security Template (Automatisch) |
| 5783 | Sekundäre Anmeldung<br>Ermöglicht das Starten von Prozessen unter Verwendung alternativer Anmeldeinformationen. Wenn dieser Dienst beendet wird, wird diese Art der Anmeldung nicht mehr zur Verfügung stehen. Wenn dieser Dienst deaktiviert wird, werden alle von diesem Dienst explizit abhängigen Dienste nicht gestartet werden können. | Secondary Logon<br>Disabled | 💣 | Security Template (Automatisch) |
| 5784 | Sicherheitskontenverwaltung<br>Speichert Sicherheitsinformationen für lokale Benutzerkonten. | Security Accounts Manager<br>Automatic | 💣 | Security Template (Automatisch) |
| 5785 | Server<br>Unterstützt Datei-, Drucker- und Named-Piped-Freigabe für diesen Computer über das Netzwerk. Diese Funktionen sind nicht mehr verfügbar, falls dieser Dienst beendet wird. Falls dieser Dienst deaktiviert wird, können die Dienste, die von diesem Dienst ausschließlich abhängig sind, nicht mehr gestartet werden. | Server<br>Automatic | 💣 | Security Template (Automatisch) |
| 5786 | Shellhardwareerkennung<br>Automatischer Start von Applikationen, die von Hardware Events ausgehen. (z.B. Bildviewer beim Einstecken von USB Massstorage) | Shell Hardware Detection<br>Disabled | 💣💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5787 | SMTP Service<br>Bildet zusammen mit dem POP Server ein Mailserver. Kann auch als Relay benutzt werden. | Simple Mail Transport Protocol (SMTP)<br>Disabled | 💣💣 | Security Template (Automatisch) |
| 5788 | Einfache TCP/IP Dienste<br>Implementiert Echo, Discard, Character Generator, Daytime und Quote of the Day Protokolle. | Simple TCP/IP Services<br>Disabled | 💣💣 | Security Template (Automatisch) |
| 5789 | SIS (Single Instance Storage Groveler)<br>Ist eine integrale Komponente vom RIS. Dieser Dienst sucht ein RIS volume nach doppelten Files ab und konsolidiert diese. | Single Instance Storage Groveler<br>Disabled | 💣 | Security Template (Automatisch) |
| 5790 | Smartcard<br>Verwaltet den Zugriff auf Smartcards, die von diesem Computer gelesen werden. Wenn dieser Dienst beendet wird, wird dieser Computer keine Smartcards mehr lesen können. Wenn dieser Dienst deaktiviert wird, werden alle von diesem Dienst explizit abhängigen Dienste nicht gestartet werden können. | Smart Card<br>Disabled | 💣 | Security Template (Automatisch) |
| 5791 | SNMP Dienst<br>Das Simple Network Management Protokol wird vor allem zum Austausch von Statusmeldungen eingesetzt. Es können auch Konfigurationsänderungen vorgenommen werden. Viele Systemmanagment Programme (HP TopTools, Compaq Insight Manager usw.) basieren auf diesem Protokoll. | SNMP Service<br>Not defined<br>→ Kann ev. Disabled werden, sofern keine Management Software eingesetzt wird. | 💣💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5792 | Konfiguration von SNMP | Folgende Parameter sind zu konfigurieren:<br>• Community name (kein default wert nehmen)<br>• Trap destination (nur mangement stationen eintragen)<br>• Security: Rechte der Communtiys<br>• Security: Eingrenzen welche Maschinen SNMP anfragen schicken dürfen | 💣💣 | Manueller Eingriff (Contol Panel-Services-SNMP Service-Properties) |
| 5793 | SNMP Trap Service | SNMP Trap Service<br>Not defined<br>→ Kann ev. Disabled werden, sofern keine Management Software eingesetzt wird. | 💣💣 | Security Template (Automatisch) |
| 5794 | SQLAgent$ (UDDI or WebDB) | SQLAgent$ (UDDI or WebDB)<br>Disabled | 💣💣 | Security Template (Automatisch) |
| 5795 | Systemereignisbenachrichtigung<br>Verfolgt Systemereignisse wie Windows-Anmeldungen sowie Netzwerk- und Stromversorgungsereignisse. Benachrichtigt außerdem COM+ Ereignissystembezieher von diesen Ereignissen. | System Event Notification<br>Automatic | - | Security Template (Automatisch) |
| 5796 | Taskplaner<br>Ermöglicht einem Benutzer, automatische Vorgänge auf diesem Computer zu konfigurieren und zu planen. Wenn dieser Dienst beendet wird, werden diese Vorgänge nicht zu den geplanten Zeiten ausgeführt werden. Wenn dieser Dienst deaktiviert wird, werden alle von diesem Dienst explizit abhängigen Dienste nicht gestartet werden können. | Task Scheduler<br>Disabled<br>→ Wird benötigt, wenn ntbackup eingesetzt wird. | 💣💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5797 | TCP/IP-NetBIOS-Hilfsprogramm<br>Ermöglicht die Unterstützung vom NetBIOS-über-TCP/IP-Dienst (NetBT) und die NetBIOS-Namensauflösung. | TCP/IP NetBIOS Helper<br>Automatic | - | Security Template (Automatisch) |
| 5798 | TCP/IP Print Server | TCP/IP Print Server<br>Disabled | 💣 | Security Template (Automatisch) |
| 5799 | Telefonie<br>Bietet Telefonie-API-Unterstützung (TAPI) für Programme, die Telefoniegeräte steuern, sowie IP-basierte Sprachverbindungen am lokalen Computer und über das LAN, auf Servern, die diesen Dienst ebenfalls ausführen. | Telephony<br>Disabled | 💣 | Security Template (Automatisch) |
| 5800 | Telnet<br>Ermöglicht einem Remotebenutzer, sich an diesem Computer anzumelden und Programme auszuführen. Unterstützt verschiedene TCP/IP-Telnetclients, einschließlich UNIX-basierten und Windows-basierten Computern. Wenn dieser Dienst angehalten wird, ist der Remotezugriff möglicherweise nicht mehr verfügbar. Wenn dieser Dienst deaktiviert wird, können alle Dienste, die explizit von diesem Dienst abhängen, nicht mehr gestartet werden. | Telnet<br>Disabled | 💣💣💣 | Security Template (Automatisch) |
| 5801 | Terminal Server Session Directory | Terminal Server Session Directory<br>Disabled | 💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5802 | Terminaldienste<br>Ermöglicht mehreren Benutzern das Herstellen interaktiver Verbindungen mit anderen Computern, sowie das Anzeigen von Desktop und Anwendungen auf Remotecomputern. Terminaldienste bilden die Grundlage für Remotedesktops (einschließlich RD für Administratoren), schnelle Benutzerumschaltung, Remoteunterstützung und Terminalserver. | Terminal Services<br>Automatic | - | Security Template (Automatisch) |
| 5803 | Designs<br>Stellt die Designverwaltung zur Verfügung. | Themes<br>Disabled | 💣 | Security Template (Automatisch) |
| 5804 | Tivial FTP Deamon | Tivial FTP Deamon<br>Disabled<br>→ Wird im Zusammenhang mit RIS verwendet! | 💣💣 | Security Template (Automatisch) |
| 5805 | Unterbrechungsfreie Stromversorgung<br>Verwaltet eine an den Computer angeschlossene unterbrechungsfreie Stromversorgung (USV). | Uninterruptible Power Supply<br>Disabled | - | Security Template (Automatisch) |
| 5806 | Upload-Manager<br>Verwaltet synchrone und asynchrone Dateiübertragungen zwischen Clients und Servern im Netzwerk. Synchrone und asynchrone Dateiübertragungen zwischen Clients und Servern werden nicht ausgeführt, wenn dieser Dienst beendet wird. Falls dieser Dienst deaktiviert wird, können die Dienste, die von diesem Dienst ausschließlich abhängig sind, nicht mehr gestartet werden. | Upload Manager<br>Disabled | 💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5807 | Verwaltung logischer Datenträger<br>Erkennt und überwacht neue Festplattenlaufwerke und sendet Festplatteninformationen zur Konfiguration an den Verwaltungsdienst für die Verwaltung logischer Datenträger. Wenn dieser Dienst beendet wird, können Statusinformationen für dynamische Festplatten und Konfigurationsinformationen veraltet oder ungültig werden. Wenn dieser Dienst deaktiviert wird, werden alle von diesem Dienst explizit abhängigen Dienste nicht gestartet werden können. | Virtual Disk Service<br>Disabled | 💣 | Security Template (Automatisch) |
| 5808 | Volumeschattenkopie<br>Verwaltet und implementiert Volumeschattenkopien, die zu Sicherungs- und anderen Zwecken verwendet werden. Wenn dieser Dienst beendet wird, werden keine Schattenkopien für Sicherungen verfügbar sein und die Sicherung kann eventuell fehlschlagen. Wenn dieser Dienst deaktiviert wird, werden alle von diesem Dienst explizit abhängigen Dienste nicht gestartet werden können. | Volume Shadow Copy<br>Manual | - | Security Template (Automatisch) |
| 5809 | Web Element Manager | Web Element Manager<br>Disabled | 💣 | Security Template (Automatisch) |
| 5810 | WebClient<br>Ermöglicht Windows-basierten Programmen, Internet-basierte Dateien zu erstellen, darauf zuzugreifen und sie zu verändern. Wenn dieser Dienst beendet wird, werden diese Funktionen nicht mehr zur Verfügung stehen. Wenn dieser Dienst deaktiviert wird, werden alle von diesem Dienst explizit abhängigen Dienste nicht gestartet werden können. | WebClient<br>Disabled | 💣💣 | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5811 | Windows Audio<br>Verwaltet Audiogeräte für Windows-basierte Programme. Wenn dieser Dienst beendet wird, werden Audiogeräte und -effekte nicht korrekt funktionieren. Wenn dieser Dienst deaktiviert wird, werden alle von diesem Dienst explizit abhängigen Dienste nicht gestartet werden können. | Windows Audio<br>Disabled | 💣 | Security Template (Automatisch) |
| 5812 | Windows-Bilderfassung (WIA)<br>Bietet Bilderfassungsdienste für Scanner und Kameras. | Windows Image Acquisition (WIA)<br>Disabled | 💣 | Security Template (Automatisch) |
| 5813 | Windows Installer<br>Installiert, repariert oder entfernt Software gemäß der in MSI-Dateien enthaltenen Anweisungen. | Windows Installer<br>Automatic | - | Security Template (Automatisch) |
| 5814 | Windows Internet Name Service (WINS) | Windows Internet Name Service (WINS)<br>Disabled | 💣 | Security Template (Automatisch) |
| 5815 | Windows Management Instrumentation Driver | Windows Management Instrumentation Driver Extensions<br>Manual | - | Security Template (Automatisch) |
| 5816 | Windows-Verwaltungsinstrumentation<br>Bietet eine standardmäßige Schnittstelle und Objektmodell zum Zugreifen auf Verwaltungsinformationen über das Betriebssystem, Geräte, Anwendungen und Dienste. Die meiste Windows-basierte Software kann nicht ordnungsgemäß ausgeführt werden, falls dieser Dienst beendet wird. Falls dieser Dienst deaktiviert wird, können die Dienste, die von diesem Dienst ausschließlich abhängig sind, nicht mehr gestartet werden. | Windows Management Instrumentation<br>Automatic | - | Security Template (Automatisch) |

| Nr. | Service/Beschreibung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5817 | Windows Media Services | Windows Media Services<br>Disabled | 💣 | Security Template (Automatisch) |
| 5818 | Windows System Resource Manager | Windows System Resource Manager<br>Disabled | 💣 | Security Template (Automatisch) |
| 5819 | Windows-Zeitgeber<br>Verwaltet die Datum- und Uhrzeitsynchronisierung auf allen Clients und Servern im Netzwerk. Wenn dieser Dienst beendet wird, ist die Datum- und Uhrzeitsynchronisierung nicht verfügbar. Wenn der Dienst deaktiviert wird, können alle anderen Dienste, die explizit davon abhängen, nicht gestartet werden. | Windows Time<br>Automatic | - | Security Template (Automatisch) |
| 5820 | WinHTTP Web Proxy Auto – Discovery Service | WinHTTP Web Proxy Auto – Discovery Service<br>Disabled | 💣💣 | Security Template (Automatisch) |
| 5821 | Konfigurationsfreie drahtlose Verbindung<br>Bietet automatische Konfiguration für 802.11-Adapter. | Wireless Configuration<br>Disabled | 💣💣 | Security Template (Automatisch) |
| 5822 | WMI-Leistungsadapter<br>Bietet Leistungsbibliotheksinformationen der WMI-HiPerf-Anbieter. | WMI Performance Adapter<br>Manual | 💣 | Security Template (Automatisch) |
| 5823 | Arbeitsstationsdienst<br>Erstellt und wartet Clientnetzwerkverbindungen mit Remoteservern. Diese Verbindungen sind nicht mehr verfügbar, falls dieser Dienst beendet wird. Falls dieser Dienst deaktiviert wird, können die Dienste, die von diesem Dienst ausschließlich abhängig sind, nicht mehr gestartet werden. | Workstation<br>Automatic | - | Security Template (Automatisch) |
| 5824 | World Wide Web Publishing Service | World Wide Web Publishing Service<br>Disabled | 💣💣 | Security Template (Automatisch) |

## 5.8 Additional Registry Settings

Leider können nicht alle Sicherheitseinstellungen über den Policy Editior eingestellt werden. Die folgenden Einstellungen sind im Security Template enthalten. Sollen die Einstellungen entfernt oder geändert werden, muss dies mittels eines Texteditors geschehen.

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5825 | Sicherheitsmassnahmen bezüglich Netzwerkattacken | EnableICMPRedirect = 0<br>SynAttackProtect = 1<br>EnableDeadGWDetect = 0<br>EnablePMTUDiscovery = 0<br>KeepAliveTime = 300000<br>DisableIPSourceRouting = 2<br>TcpMacConnectResponseRetransmissions = 2<br>TcpMaxDataRetransmissions = 3<br>PerformRouterDiscovery = 0<br>TCPMaxPortsExhausted = 5 | 💣💣 | Security Template (Automatisch) |
| 5826 | AFD.SYS Einstellungen | DynamicBacklogGrowthDelta = 10<br>EnableDynamicBacklog = 1<br>MinimumDynamicBacklog = 20<br>MaximumDynamicBacklog = 20000 | 💣💣 | Security Template (Automatisch) |
| 5827 | Allow the computer to ignore NetBIOS name release requests except from WINS servers | NoNameReleaseOnDemand = 1 | 💣💣 | Security Template (Automatisch) |
| 5828 | Auschalten der 8.3-Namenserstellung | NtfsDisable8dot3NameCreation = 1 | 💣💣 | Security Template (Automatisch) |
| 5829 | Ausschalten der Autorun-Funktion auf allen Laufwerken | NoDriveTypeAutoRun = 0xFF | 💣💣💣 | Security Template (Automatisch) |
| 5830 | Einschalten des sofortigen Passwortschutzes des Bildschirmschoners | ScreenSaverGracePeriod = 0 | 💣💣 | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5831 | Einschalten des sicheren DLL Suchmodus | SafeDllSearchMode = 1 | 💣💣💣 | Security Template (Automatisch) |

## 5.9 Additional Security Settings

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5900 | Internet Explorer: Disable Automatic Install of IE components | Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Disable Automatic Install of Internet Explorer components Enabled | 💣💣💣 | Manueller Eingriff<br>Group Policy Object Editor |
| 5901 | Internet Explorer: Disable Periodic Check for IE software updates | Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Disable Automatic Install of Internet Explorer updates | 💣💣💣 | Manueller Eingriff<br>Group Policy Object Editor |
| 5902 | Keine Fehlerberichte sollen an Microsoft gesendet werden | Report Errors = Disabled<br>→ Group Policy Path:<br>Computer Configuration\Administrative Templates\System\Error Reporting | 💣💣💣 | Manueller Eingriff<br>Group Policy Object Editor |
| 5903 | Logon: Do not process the legacy run list | Computer Configuration\Administrative Templates\System\Logon\Do not process the legacy run list<br>Not defined | 💣💣💣 | Manueller Eingriff<br>Group Policy Object Editor |
| 5904 | Logon: Do not process the run once list | Computer Configuration\Administrative Templates\System\Logon\Do not process the run once list<br>Not defined | 💣💣💣 | Manueller Eingriff<br>Group Policy Object Editor |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5905 | NetMeeting: Disable remote Desktop Sharing | Computer Configuration\Administrative Templates\Windows Components\NetMeeting\Disable remote Desktop Sharing Enabled | 💣💣💣 | Manueller Eingriff<br>Group Policy Object Editor |
| 5906 | Terminal Services: Allow audio redirection | Set setting to Disabled.<br>→ Group Policy Path:<br>Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection | 💣💣 | Manueller Eingriff<br>Group Policy Object Editor |
| 5907 | Terminal Services: Do not allow COM port redirection | Set setting to Enabled.<br>→ Group Policy Path:<br>Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection | 💣💣 | Manueller Eingriff<br>Group Policy Object Editor |
| 5908 | Terminal Services: Do not allow drive redirection | Set setting to Enabled.<br>→ Group Policy Path:<br>Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection | 💣💣💣 | Manueller Eingriff<br>Group Policy Object Editor |
| 5909 | Terminal Services: Do not allow LPT port redirection | Set setting to Enabled.<br>→ Group Policy Path:<br>Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection | 💣💣 | Manueller Eingriff<br>Group Policy Object Editor |
| 5910 | Terminal Services: Do not allow printer redirection | Set setting to Enabled.<br>→ Group Policy Path:<br>Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection | 💣💣 | Manueller Eingriff<br>Group Policy Object Editor |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 5911 | Terminal Services: Do not allow smart card device redirection | Set setting to Enabled.<br>→ Group Policy Path:<br>Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection | 💣💣 | Manueller Eingriff<br>Group Policy Object Editor |
| 5912 | Terminal Services: Do not set default client printer to be default printer in a session | Set setting to Enabled.<br>→ Group Policy Path:<br>Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection | 💣💣 | Manueller Eingriff<br>Group Policy Object Editor |
| 5913 | Verschlüsselungsstärke bei Terminal Services | Set client connection encryption level = High<br>→ Group Policy Path:<br>Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security | 💣💣 | Manueller Eingriff<br>Group Policy Object Editor |
| 5914 | Windows Media Player: Prevent Automatic Updates | Computer Configuration\Administrative Templates\Windows Components\Windows Media Player\Prevent Automatic Updates Enable | 💣💣💣 | Manueller Eingriff<br>Group Policy Object Editor |
| 5915 | Windows Messenger: Do not allow Windows Messenger to be run | Computer Configuration\Administrative Templates\Windows Components\Windows Messenger\Do not allow Windows Messenger to be run Enabled | 💣💣💣 | Manueller Eingriff<br>Group Policy Object Editor |
| 5916 | Windows Messenger: Do not automatically start Windows Messenger initially | Computer Configuration\Administrative Templates\Windows Components\Windows Messenger\Do not automatically start Windows Messenger initially Enabled | 💣💣💣 | Manueller Eingriff<br>Group Policy Object Editor |

# 6 Hardening Domain Controller (ADS)

| Wirkungskreis | Anwendung | Compass Template Name |
|---|---|---|
| Dieses Kapitel beschreibt die Sicherheitseinstellungen auf den Domain Controllern. | **Zuerst** wird die INF-Datei des Memberservers gemäss Kapitel 7.1 appliziert. **Darauf folgend** wird das INF-File des Domain Controllers auf die gleich Weise mit „Import Policy“ appliziert. | Intranet_Baseline_Security_Domain_CSNC_V1.2.inf |

Da das Hardening des Domain Controllers auf demjenigen des Member Servers basiert, wird untenstehend wird nur die Differenz zum Kapitel 5 “Hardening Member Server” aufgezeigt.

## 6.1 Installation

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 6100 | Keine Standard-Verzeichnisse wählen | Z.b c:\win2k3 und c:\win2k3\ads | 💣 | Manueller Eingriff |
| 6101 | NTFS für alle Dateisysteme einsetzen | Damit Berechtigungen vergeben können, müssen alle Partitionen mit NTFS formatiert werden. Bestehende FAT Partitionen können mittels `convert` konvertiert werden. | 💣💣 | Manueller Eingriff |
| 6102 | Konfiguration der Länder- und Zeiteinstellung | Deutsch (Schweiz) und entsprechende Zeitzone während der Installation auswählen | 💣 | Manueller Eingriff |
| 6103 | Keine Installation von Client-Software (z.B. Outlook, Word, Excel…) auf dem Server | Auf dem Server sollen keine Officearbeiten erledigt werden. Auch das Surfen im Internet soll weitmöglichst eingegrenzt werden. | 💣💣 | Manueller Eingriff |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 6104 | Aufteilung der Programme und Daten auf separate Partitionen | Die Daten (z.B Webroot bei einem IIS) sollten auf eine separate Partition verschoben werden. | 💣💣 | Manueller Eingriff |
| 6105 | Keine Installation von Applikationen auf Domain Controller | Auf DC's sollten keine Applikationen wie IIS, SQL usw. installiert werden. Da diese die Sicherheit massiv gefährden könnten. | 💣💣💣 | Manueller Eingriff |
| 6106 | Entfernen von unnötigen Programmen | Entfernen von:<br>• Aktualisierung von Stammzertifikaten<br>• MSN Explorer<br>• Netzwerkdienste<br>• Outlook Express<br>• Windows Messenger<br><br>Danach sind nur noch folgende Komponenten aktiv: Indexdienst, Internet Explorer, Windows Media Player und einige Zubehör- und Dienstprogramme. | 💣💣 | Manuell – Systemsteuerung – Software<br><br>PS: Zusätzliche Komponenten können entfernt werden, werden aber in der Ansicht versteckt. Um das zu Umgehen editiert man die Datei C:\Windows\inf\sysoc.inf und entfernt überall das Wort HIDE. |

## 6.2 System Configuration

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 6200 | Installation des aktuellsten Service Packs | Siehe http://www.microsoft.com/technet/security/tpsrvpck.asp und http://www.microsoft.com/technet/security/current.asp | 💣💣💣 | Manueller Eingriff |
| 6201 | Konfiguration des automatischen Updates für betriebssystembasierte Hoffixes | Benutzung von SUS. Siehe Kapitel 7.5.2 | 💣💣💣 | Manueller Eingriff |
| 6202 | Konfiguration der domänenweiten Zeitsynchronisation | Siehe Kapitel 7.1 | 💣💣 | Manueller Eingriff |
| 6203 | Einschalten des Remote Desktop Zugriffes | Rechts Klick auf „My Computer“ und den Tab Remote auswählen. Danach „Allow users to connect remotely tho this computer“ auswählen. Unter “Select Remote Users” alle unerwünschten Accounts entfernen. | - | Manueller Eingriff |
| 6204 | Installation und Konfiguration eines Virenscanners | Installation eines Virenscanners der das neue API z.b Norton 8.1) von Windows 2003 benutzt. Konfiguration von regelmässigen Updates (min. 1 mal täglich) | 💣💣💣 | Manueller Eingriff |

## 6.3 User Rights Assignments

In der folgenden Liste taucht oft „Not defined“ auf. Administratoren erhalten automatisch alle Privilegien die auf „Not defined“ gesetzt sind. Lokale Administratoren können dies ändern. Dies wird jedoch, falls definiert, von der domänenweiten Policy wieder überschrieben.

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 6300 | Auf diesen Computer vom Netzwerk aus zugreifen | Access this computer from the network<br>Not Defined | 💣💣 | Security Template (Automatisch) |
| 6301 | Hinzufügen von Arbeitsstationen zur Domäne | Add workstations to domain<br>Administrators | 💣 | Security Template (Automatisch) |
| 6302 | Lokal anmelden | Allow log on locally<br>Administrators | 💣💣 | Security Template (Automatisch) |
| 6303 | Anmeldung über Terminaldienste zulassen | Allow log on through Terminal Services<br>Administrators | 💣💣 | Security Template (Automatisch) |
| 6304 | Ändern der Systemzeit | Change the system time<br>Administrators | 💣 | Security Template (Automatisch) |
| 6305 | Zugriff vom Netzwerk auf diesen Computer verweigern | Deny access to this computer from the network<br>Anonymous Logon | 💣💣 | Security Template (Automatisch) |
| 6306 | Anmeldung als Batchauftrag verweigern | Deny log on as a batch job<br>Guest | 💣💣 | Manueller Eingriff |
| 6307 | Anmeldung über Terminaldienste verweigern | Deny log on through Terminal Services<br>Built-in Administrator, Support_388946a0, all NON-Operating System service accounts (e.g Exchange, SQL…) | 💣💣 | Manueller Eingriff |
| 6308 | Enable computer and user acconts to be trusted for delegation | Enable computer and user acconts to be trusted for delegation<br>Not defined | 💣💣 | Security Template (Automatisch) |

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 6309 | Laden und Entfernen von Gerätetreibern | Load and unload device drivers<br>Administrators | 💣 | Security Template (Automatisch) |
| 6310 | Wiederherstellen von Dateien und Verzeichnissen | Restore files and directories<br>Administrators | 💣 | Security Template (Automatisch) |
| 6311 | Herunterfahren des Systems | Shut down the system<br>Administrators | 💣 | Security Template (Automatisch) |

## 6.4 Security Options

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 6400 | Konten: Administrator umbenennen | Accounts: Rename administrator account<br>Droot (Domain Root) | 💣 | Manueller Eingriff |
| 6401 | Netzwerksicherheit: Keine LAN Manager-Hashwerte für nächste Kennwortänderung speichern | Network security: Do not store LAN Manager hash value on next password change<br>Enabled<br>→ Alle Passwörter müssen neu vergeben werden. Diese Einstellung gilt nur für neue Passwörter! | 💣💣 | Security Template (Automatisch) |

## 6.5 System Services

| Nr. | Service | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 6500 | Distributed File System | Distributed File System<br>Automatic | - | Security Template (Automatisch) |
| 6501 | DNS Server | DNS Server<br>Automatic | - | Security Template (Automatisch) |
| 6502 | DHCP-Server<br>Stellt die dynamische Netzwerkkonfiguration zur Verfügung, indem IP-Adressen und DNS-Namen an DHCP-Clients verteilt werden. | DHCP Server<br>Automatic | 💣 | Security Template (Automatisch) |
| 6503 | File Replication | File Replication<br>Automatic | - | Security Template (Automatisch) |
| 6504 | Intersite Messaging | Intersite Messaging<br>Automatic | - | Security Template (Automatisch) |
| 6505 | Kerberos Key Distribution Center | Kerberos Key Distribution Center<br>Automatic | - | Security Template (Automatisch) |
| 6506 | Remote Procedure Call (RPC) Locator | Remote Procedure Call (RPC) Locator<br>Automatic | - | Security Template (Automatisch) |
| 6507 | Windows Internet Name Service (WINS) | Windows Internet Name Service (WINS)<br>Automatic<br><br>Wird beim Einsatz von NT4 Computern noch benötigt. | 💣 | Security Template (Automatisch) |

## 6.6 Additional Security Settings

| Nr. | Sicherheitseinstellung | Empfehlung | Gewichtung | Referenz |
|---|---|---|---|---|
| 6600 | Internet Information Services: Prevent IIS Installation | Computer Configuration\Administrative Templates\Windows Components\Internet Information Services\Prevent IIS Installation Enabled | | Manueller Eingriff<br>Group Policy Object Editor |

# 7 Anhang

## 7.1 Security Templates

Security Templates sind Textdateien, die mittels des Security Templates Snap-in (MMC) oder einem Editor bearbeitet werden können. Bei der Definition von Zugriffberechtigungen wird die so genannte Security Descriptor Definition Language (SDDL) benutzt. Weiterführende Informationen finden sich unter: http://msdn.microsoft.com/library/en-us/kmarch/hh/kmarch/devobjts_5e07.asp

Es werden mit dem Betriebssystem schon vordefinierte Security Templates mitgeliefert. Diese finden sich im %SystemRoot%\security\templates Verzeichnis. Es ist unbedingt darauf zu achten, dass die benutzen Templates nicht verändert werden können. Normale Benutzer haben aus diesem Grund „nur“ Leseberechtigungen auf diesem Verzeichnis.

### 7.1.1 Default Templates

Mit den Default Templates können jederzeit die ursprünglichen Sicherheitseinstellungen wiederhergestellt werden.

- Windows 2003 Server: %windir%\inf\defltsv.inf
- Windows 2003 Domain Controller: %windir%\inf\defltdc.inf

Vorgegangen wird dabei wie im Q266118 beschrieben (Siehe Mircrosoft Knowledgebase).

### 7.1.2 Import von Security Templates (Standard)

**Es wird empfohlen die neue Group Policy Management Console für das hantieren mit Group Policies zu benutzen (siehe Kapitel 7.1.3).**

**ACHTUNG!!!**

- Es ist unbedingt darauf zu achten, dass keine Templates verwechselt werden. Ansonsten funktionieren einige Dienste nicht mehr.
- Die von Compass Security modifizierten Templates sind im Labor getestet worden. Jedoch könnten einige Einstellungen die Funktion von Anwendungen beeinträchtigen. Wo solche Restriktionen bekannt sind, ist in der jeweiligen Beschreibung eine Bemerkung gemacht. Aus diesen Gründen wird dringest empfohlen diese Checkliste zuerst durch zu lesen und etweilige Punkte anzupassen.

Folgen Sie den Anweisungen um ein Security Template in eine OU zu importieren:

1. Klicken Sie mit der rechten Maustaste auf den entsprechenden OU-Container in „Active Directory Users and Computers“ und wählen Sie „Properties“.
2. Wählen Sie auf den „Group Policy“ Tab neu um eine neue GPO anzulegen.
3. Benennen Sie die Policy (z.B. Intranet Baseline Domain Policy)

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

4. **Dieser Schritt sollte nur bei der Domain Policy vorgenommen werden!**
   Klicken Sie mit der rechten Maustaste auf das soeben angelegte Objekt und wählen Sie „No Override“.
5. Wählen Sie das Objekt an und klicken Sie Edit.
6. Klicken Sie auf Computer Configuration-Windows Settings im Group Policy Object Editor. Nach einem Rechtsklick auf Security Settings wählen Sie “Import Policy”.
7. Wählen Sie nun das ensprechende Template aus.
8. Die Einstellungen sind nun importiert worden und es können alle Fenster geschlossen werden.
9. Wenn gewünscht kann die Replizierung der Policy auf die anderen Domain Controller mittels des Commandline-Tools gpupdate.exe forciert werden. Dazu muss auf den entsprechenden Maschinen der Befehl gpupdate /force eingegeben werden. Auf dieselbe Weise kann bei einem Windows XP Client die Policy neu angewendet werden.
10. Im Event Log sollten entsprechende Einträge zu finden sein.


**ACHTUNG!!!**

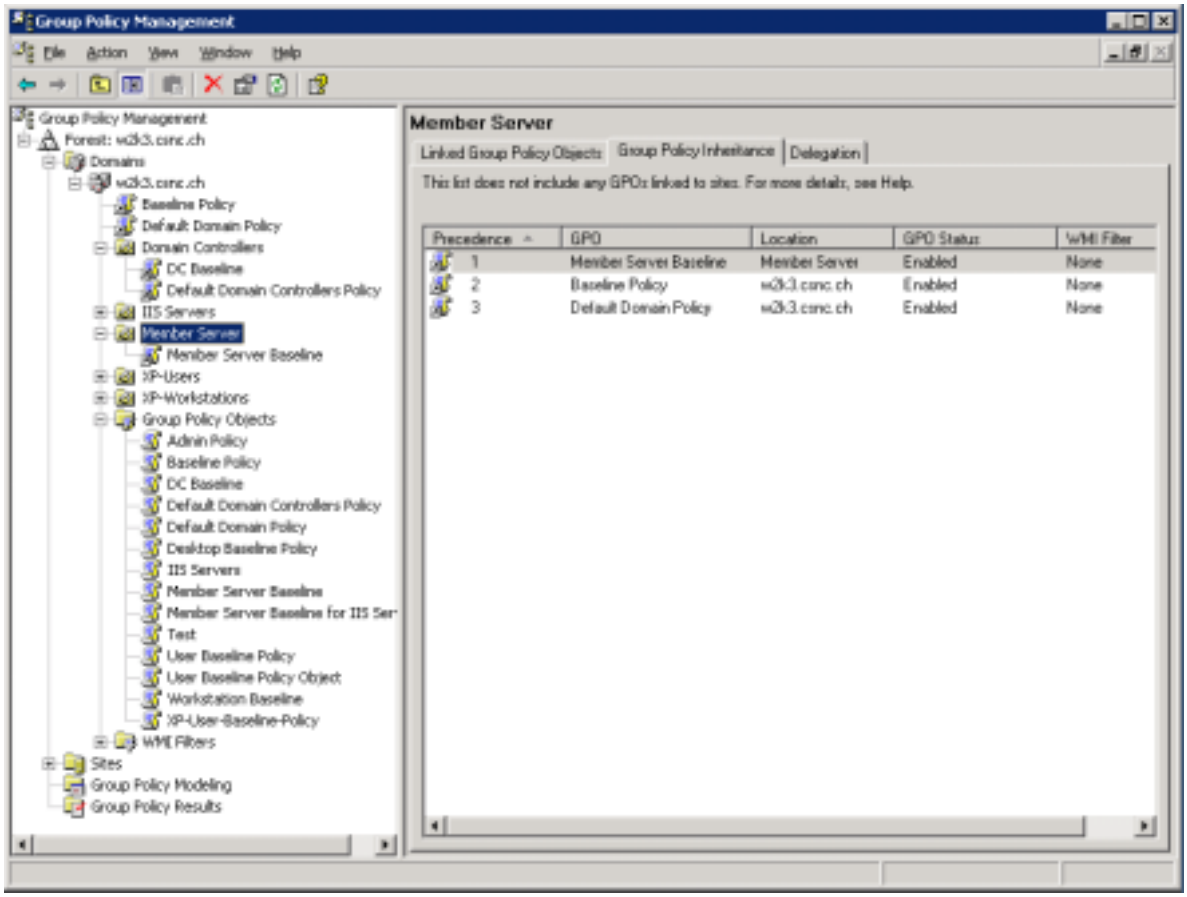
- Die „No Override“ Einstellung sollte nur bei der Domain Policy eingeschaltet werden. So wird sichergestellt, dass diese Policy für die gesamte Domain angewendet wird.
- Die „Default Domain Policy“ kann so belassen werden um nötigenfalls die Default-Einstellungen zu reaktivieren.
- Die Domain Policy sollte in jede Domain in der Unternehmung importiert werden.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

### 7.1.3 Group Policy Management Console (GPMC)

Mit GPMC wird die Verwaltung von Gruppenrichtlinien vereinfacht. Das Analysieren, Bereitstellen, Verwalten und das Behandeln von Problemen für Implementationen mit Gruppenrichtlinien werden erleichtert. GPMC ermöglicht auch das Automatisieren von Gruppenrichtlinienvorgängen mittels Skripterstellung. Die GPMC ist ein MMC Snap-in.




#### 7.1.3.1 Installation der GPMC

1. Downloaden Sie die Group Policy Management Console unter http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=F39E9D60-7E41-4947-82F5-3330F37ADFEB

2. Führen Sie zum Installieren von GPMC das Paket Gpmc.msi aus. Nachdem Sie den Endbenutzer-Lizenzvertrag (EULA) akzeptiert haben, werden alle notwendigen Dateien im Ordner %ProgramFiles%\GPMC installiert.

Nach dem Installieren von GPMC können Sie das Snap-In mit einer der folgenden Methoden öffnen:

- Öffnen der vorkonfigurierten Datei GPMC.msc. Klicken Sie dazu im Startmenü auf Ausführen, geben Sie GPMC.msc ein, und klicken Sie dann auf OK.
- Sie können auch in der Systemsteuerung im Ordner Verwaltung auf die Verknüpfung Gruppenrichtlinienverwaltung klicken.
- Erstellen einer benutzerdefinierten MMC-Konsole mit dem GPMC-Snap-In. Führen Sie dazu folgende Aktionen aus:
    - Klicken Sie zum Öffnen von MMC im Startmenü auf Ausführen, geben Sie MMC ein, und klicken Sie dann auf OK.
    - Klicken Sie im Menü Datei auf Snap-In hinzufügen/entfernen und dann auf Hinzufügen.
    - Klicken Sie im Dialogfeld Eigenständiges Snap-In hinzufügen auf Gruppenrichtlinienverwaltung, und klicken Sie dann auf Hinzufügen.
    - Klicken Sie auf Schließen und dann auf OK.

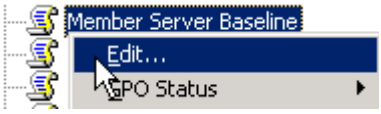
GPMC enthält mehrere Beispielskripts. Diese werden im Ordner %ProgramFiles%\GPMC\Scripts installiert. Sie sollten alle Beispielskripts mit Cscript.exe ausführen. Weitere Informationen zu Skripts finden Sie in der Datei ScriptingReadMe.rtf im Ordner Scripts. Anweisungen und Syntaxinformationen zu den einzelnen Skripts erhalten Sie, wenn Sie das jeweilige Skript mit dem /? -Parameter ausführen.

### 7.1.3.2 Neue Policy erstellen

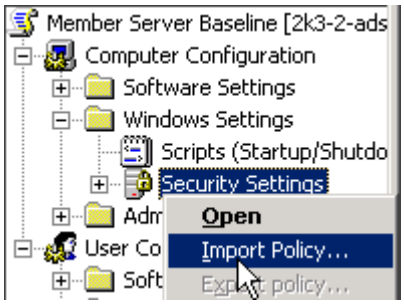
1. GPMC öffnen. Muss ev. noch installiert werden. Siehe dazu http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx


2. Neue Policy unter „Group Policy Objects“ anlegen.


3. Neu erstellte Policy im “Group Policy Object Editor” öffnen.

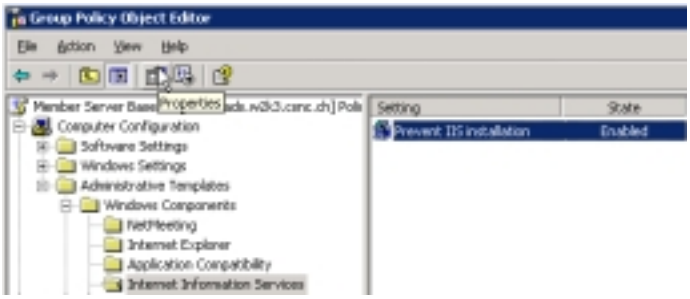



4. INF-Datei (Security Template) von Compass importieren.



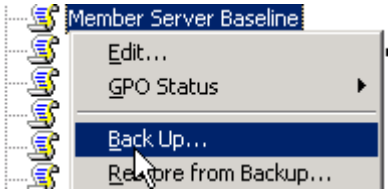

**Achtung:** Bei der Domain Controller Policy muss zuerst das Memberserver Template und danach direkt das Domain Controller Template importiert werden.

5. Manuelle Anpassungen vornehmen (Siehe Checkliste).




6. Entfernen aller „Nicht Built-in User“ sonst gibt es beim Import Fehler.

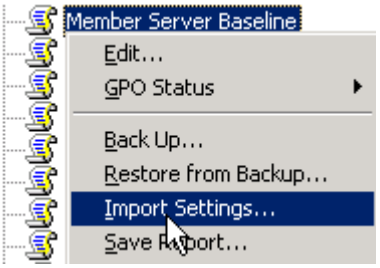
7. Backup der fertigen Policy




### 7.1.3.3 Policy Backup importieren und linken

1. Neue Policy unter „Group Policy Objects“ anlegen.


2. Importieren der gesicherten Group Policy




3. Linken der Policy


4. Löschen der Default Policies (beim erstellen von Domain- und DC-Policies)

Falls Policies für die Domäne oder für die Domänen Controller erstellt werden, können die entsprechenden Default Policies resp. deren Links gelöscht werden.

5. Priorität der Policy überprüfen

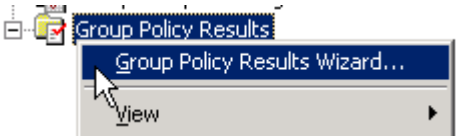

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

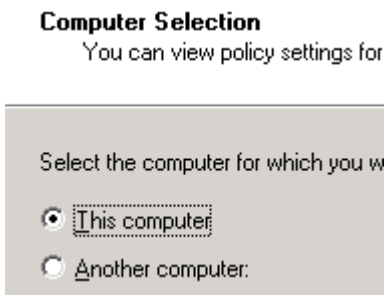
#### 7.1.3.4 Einstellungen überprüfen

Die GPMC ermöglich es einfach die angewendeten Einstellungen zu überprüfen. Um einen solchen Report zu erstellen wird folgendermassen vorgegangen:

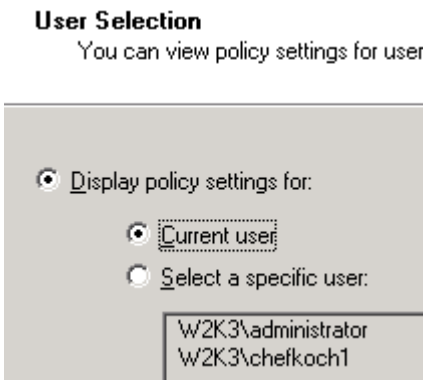
1. „Group Policy Results Wizard“ in der GPMC aufrufen.




2. Auswahl des gewünschten Computers




3. Auswahl des gewünschten Benutzers




4. Analyse der Einstellungen (Tab Settings im rechten Fenster)

## 7.1 Group Policy Tools

There are several tools that ship with Windows XP which make working with GPOs easier. A brief overview of some of these tools is provided in the following section. For more information on these tools, see the Help for Windows XP.

### 7.1.1 Forcing a Group Policy Update

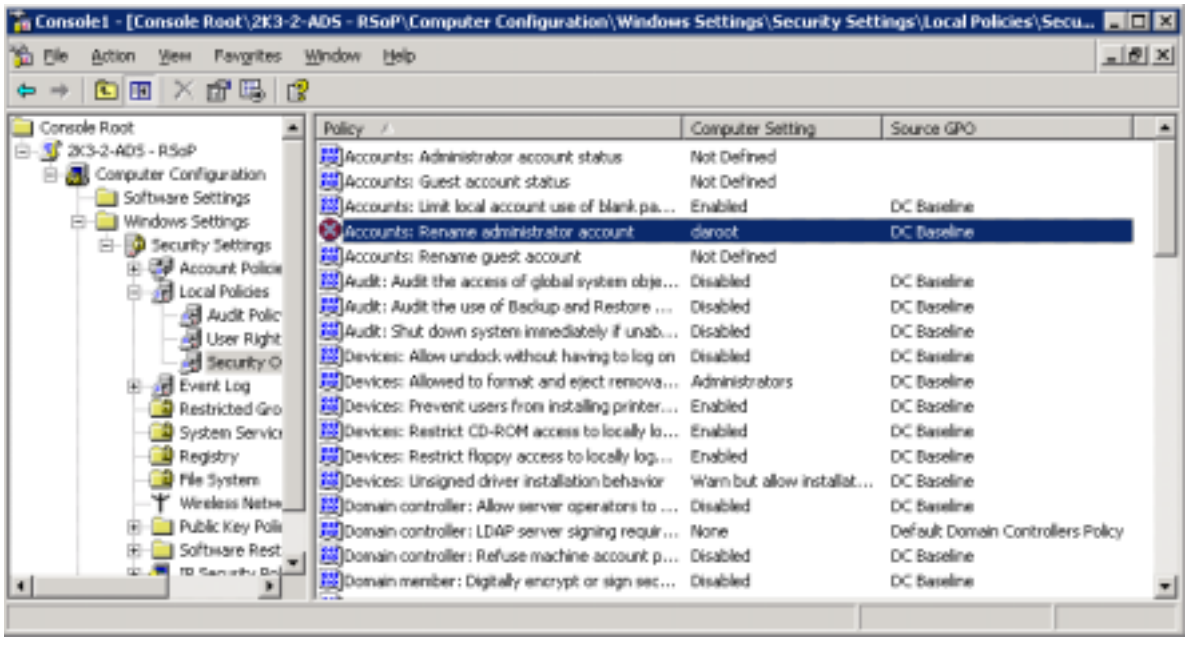
Mit dem Commandline-Tool `gpupdate.exe` kann die Anwendung der Policy auf einer Workstaion forsier werden.

```
C:\Documents and Settings\administrator.MSSLAB>gpupdate /force
Refreshing Policy...
User Policy Refresh has completed.
Computer Policy Refresh has completed.
To check for errors in policy processing, review the event log.
C:\Documents and Settings\administrator.MSSLAB>
```

Werden benutzerbasierte Policies appliziert, muss der Benutzer ab- und wieder angemeldet werden. Computerbasierte Policies werden hingegen sofort angewendet.

### 7.1.2 Viewing the Resultant Set of Policies

Mit dem MMC Snap-In RSoP.msc (Resultant Set of Policy) kann die exakte Anwendung der Policy eingesehen werden. Dasselbe kann mit dem Commandline-Tool `gpresult.exe` erreicht werden.




## 7.2 Administrative Tools

Auf einer Workstation sind die Administrativen Tools resp. die MMC Snap-ins zur Administration der Domäne nicht vorhanden. Sie können aber leicht installiert werden. Einfach auf der gewünschten Workstation die Windwos 2003 Server CD einlegen und im i386-Verzeichnis das Adminpak.msi aufrufen. Danach werden die Admin-Tools installiert und sind danach im Start-Menu unter Verwaltung zu finden.

## 7.3 Time Service

Standardmässig synchronisieren alle Domain-Member die Zeit in der Domain. Dies ist die Grundlage für das Funktionieren von Kerberos und Auswertung von Log-Dateien. Die Zeitquelle ist dabei der PDC Emulator (Operation Master) in der Forest Root Domain. Diesen sollte man mit einer genauen Zeitquelle synchronisieren (z.B. NTP Zeitserver auf dem Internet). Wenn im „Active Directory Users and Computers“ die Domäne mit der rechten Maustaste angeklickt und danach „Operational Master“ angewählt wird, werden die „Operations Masters“ für die jeweiligen Dienste angezeigt.

**Zeitsynchronisation mittels NTP über das Internet**

1. Firewall Verbindungen für die entsprechenden Maschinen (keine Any-Rule) für UDP 123 (NTP) öffnen.
2. Eingabe des folgenden Befehls auf dem Kommandoprompt
   `w32tm /config /syncfromflags:manual /manualpeerlist:time.ethz.ch,swisstime.ethz.ch`
3. Um die Zeit sofort zu synchronisieren:
   `w32tm /config /update`
4. Im Event-Log kann die Funktion nachgeprüft werden.

## 7.4 Relevante Servicepacks und Hotfixes

Siehe http://www.microsoft.com/technet/security/current.asp

| Datum | KB Artikel | Schwachstelle | Risk |
|---|---|---|---|
| January 13, 2004 | 832483 | Buffer Overrun in MDAC Function Could Allow Code Execution | 💣💣💣 |
| Nov 11, 2003 | 824145 | Cumulative Security Update for Internet Explorer | 💣💣💣 |
| Oct 15, 2003 | 824141 | Buffer Overrun in the ListBox and in the ComboBox Control Could Allow Code Execution | 💣💣💣 |
| Oct 15, 2003 | 825119 | Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise | 💣💣💣 |
| Oct 15, 2003 | 828035 | Buffer Overrun in Messenger Service Could Allow Code Execution | 💣💣💣 |
| Oct 15, 2003 | 823182 | Vulnerability in Authenticode Verification Could Allow Remote Code Execution | 💣💣💣 |
| Sep 10, 2003 | 824146 | Buffer Overrun In RPCSS Service Could Allow Code Execution | 💣💣💣 |
| Sep 3, 2003 | 824105 | Flaw in NetBIOS Could Lead to Information Disclosure | 💣 |
| Jul 23, 2003 | 819696 | Unchecked Buffer in DirectX Could Enable System Compromise | 💣💣💣 |
| Jul 9, 2003 | 823559 | Buffer Overrun In HTML Converter Could Allow Code Execution | 💣💣💣 |

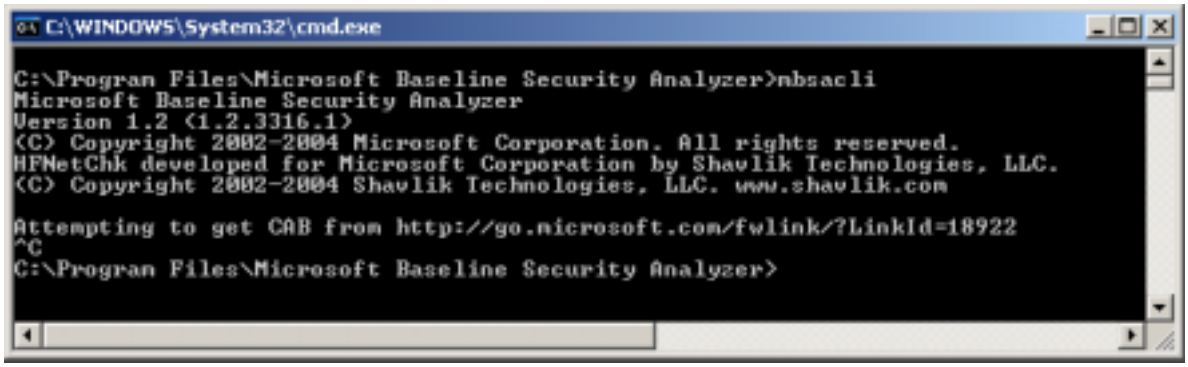
GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

| Datum | KB Artikel | Schwachstelle | Risk |
|---|---|---|---|
| Jun 25, 2003 | 819639 | Flaw In Windows Media Player May Allow Media Library Access | 💣💣 |

### 7.4.1 Automatischer Patch Check (MBSA)

Um den Patchlevel automatisch zu checken, kann der MBSA (Microsoft Baseline Security Analyzer) benutzt werden. Damit nicht das ganze Tool auf den Server installiert werden muss, kann die Commandline Variante benutzt werden. Dazu installiert man das Tool auf einer Testmaschine und kopiert lediglich mbsacli.exe auf den zu testenden Server. Nachdem Aufruf auf der Kommandozeile wird der Link der Patch-Datenbank ausgegeben:




Am besten lädt man sich die entsprechende Datei mit dem Browser herunter und entpackt das mssecure.cab File ins selbe Verzeichnis wie das mbsacli.exe.

Danach kann mittels folgendem Aufruf den Patchlevel überprüft werden:

```
C:\Program Files\Microsoft Baseline Security Analyzer>mbsacli /hf -x mssecure.xml
```

Danach wird eine Liste der fehlenden Patches ausgegeben.

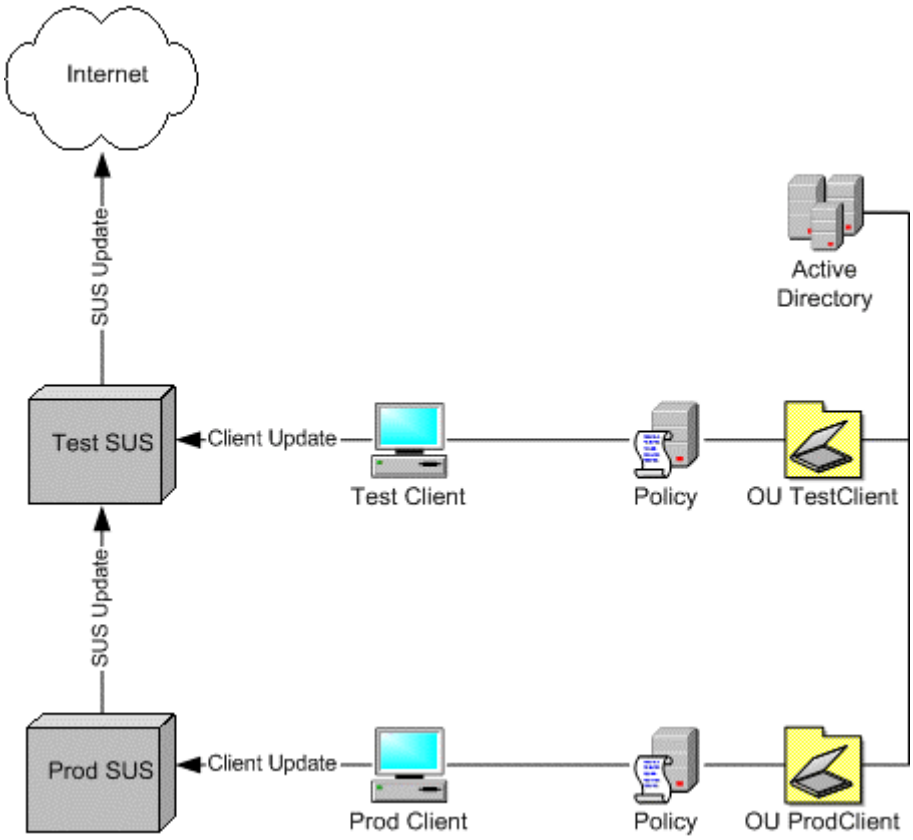
GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

## 7.5 Software Update Services (SUS)

Die Software Update Services (SUS) sind ein neues Tool, das von Microsoft zur Verwaltung und Verteilung wichtiger Windows-Patches unter Microsoft Windows 2000, Windows XP und Windows Server entwickelt wurde. Dadurch kann die Sicherheit und Stabilität von Computerumgebungen erhöht werden. Das Tool bietet die Möglichkeit, die Implementierung von Sicherheitspatches und Aktualisierungen zu automatisieren und dadurch stets einen hohen Sicherheitsstandard für Netzwerke bereitzustellen. Software Update Service erspart zeitaufwändige Recherchen im Internet sowie manuelle Downloadvorgänge und die Verteilung von Patches innerhalb der Computerumgebung.

Es wird empfohlen zwei SUS-Server aufzubauen. Einer für das Update der Testclients und Einer für das Update der produktiven Clients.




### 7.5.1 Installation und Konfiguration von SUS

Der SUS wird am besten auf einen Memberserver (Windows 2000 oder 2003) installiert. Zur Administration wird ein IIS benötigt. Automatisch wird URLScan mitinstalliert und die Adminpages per Basic Auth Passwort geschützt. Es wird empfohlen die Adminpage mit SSL zu schützen und den IIS gemäss der entsprechenden Checkliste von Compass Security zu härten. Für eine genaue

Anleitung wird auf die Dokumentation von Microsoft verwiesen.
http://www.microsoft.com/windows2000/docs/SUS_sp1_install.doc

Nach der erfolgten Installation ist das Admin-Interface des SUS auf folgendem URL erreichbar:
http://[server]/SUSAdmin/ .

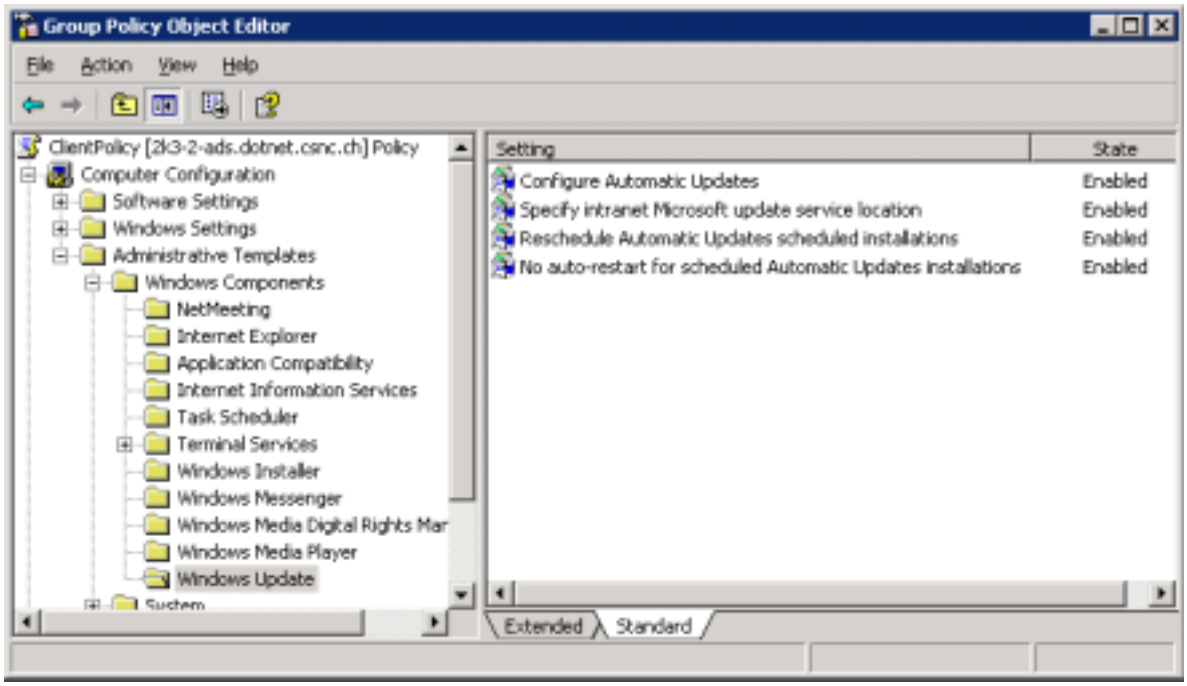
Die Konfigurations-Parameter sind unten aufgelistet:

| Parameter | Einstellung |
|---|---|
| Synchronize server-Synchronization Schedule | Synchronize using this schedule<br>At this time: 01:00<br>Daily<br>Number of synchronization retries: 3 |
| Other Options-Set options-Select a proxy server configuration | Damit dieser Server aus Ihrem Unternehmensnetz ins Internet eine Verbindung aufbauen kann, wird ev. ein Proxy benötigt. |
| Other Options-Set options-Specify the name your clients use to locate this update server | Angabe des NetBIOS-Namen des Servers (z.B. sus01) |
| Other Options-Set options-Select which server to synchronize content from | Hier wird angegeben ob dieser Server die Patches direkt vom Internet herunterlädt oder von einem anderen SUS. |
| Other Options-Set options-Select how you want to handle new versions of previously approved updates | Es wird empfohlen alle Updates von Hand zu bestätigen. |
| Other Options-Set options-Select where you want to store updates | Save the updates to a local folder<br>Die Patches sollen im lokalen Netzwerk vorhanden sein. Ansonsten müssen diese von jedem Client vom Internet herunter geladen werden. |
| Other Options-Set options-Select where you want to store updates (Languages) | Nur die benötigen Sprachen auswählen.<br>(German & English) |

### 7.5.2 Client Installation und Konfiguration (Windows Update)

Windows Update wird seit Windows 2000 mit dem Betriebsystem ausgeliefert. Beim Einsatz mit SUS wird Windows Update einfach auf den entsprechenden SUS-Server „umgebogen“. Damit Windows Update mit dem SUS SP1 funktioniert ist eine aktualisierte Version nötig. Diese liegt beim SP3 für Windows 2000, SP1 für Windows XP und bei Windows 2003 bei. Die Konfiguration kann mit einer Policy bewerkstelligt werden. Die Konfiguration für den Domänenbetrieb wird unten beschrieben. Weitere Einzelheiten können wiederum der Anleitung von Microsoft entnommen werden. http://www.microsoft.com/windows2000/docs/SUS_sp1_install.doc

Im Domänenbetrieb kann eine Group Policy erstellt werden um die benötigten Konfigurationsparameter automatisch zu verteilen. Dazu wird eine neue Organization Unit erzeugt in welche alle Workstations verschoben werden. Auf dieser OU wird dann eine Group Policy erzeugt (Rechtsklick auf die OU – Properties – Group Policy).

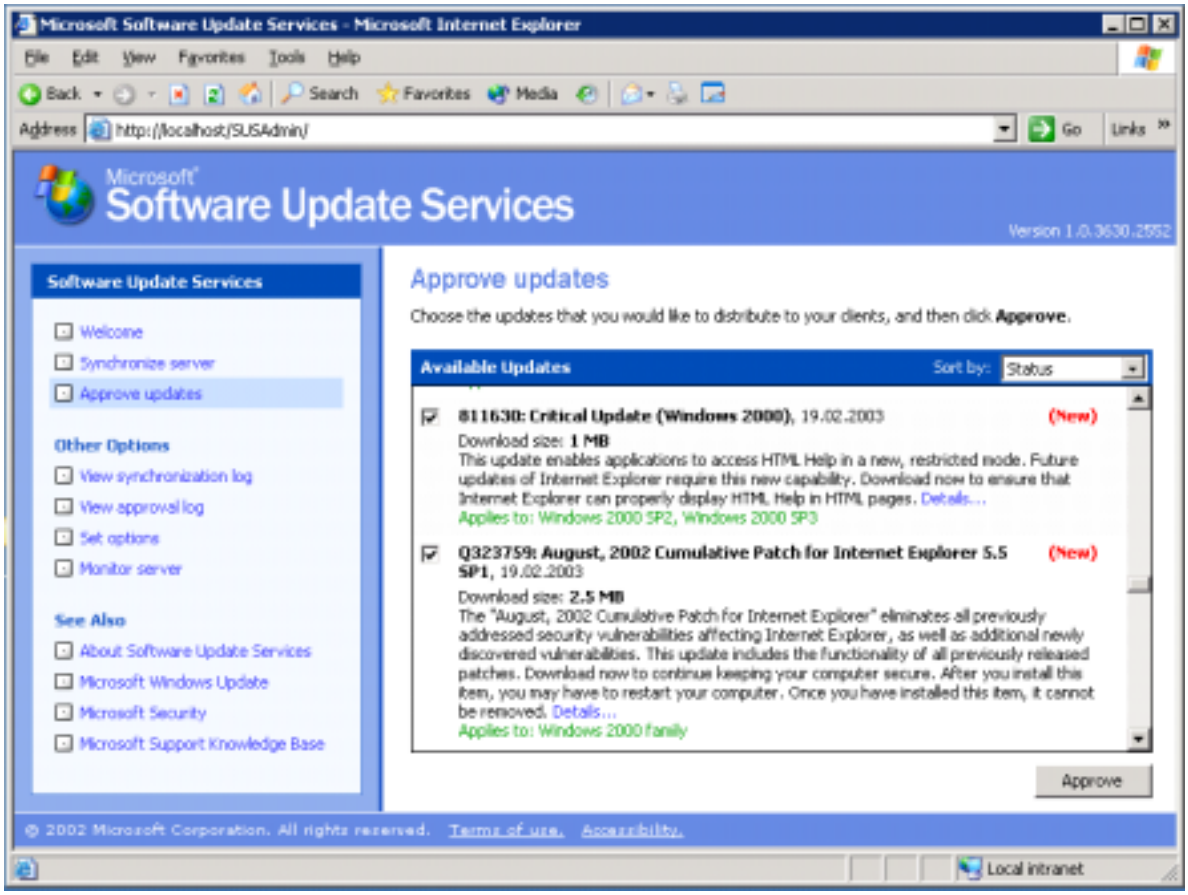



Folgende Einstellungen wurden erfolgreich getestet und als anwendbar befunden:

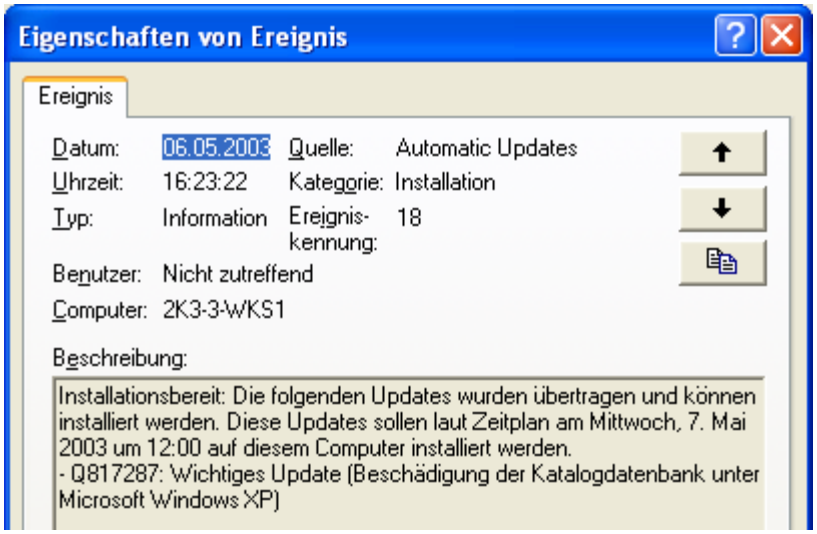
| Setting | Options | Description |
|---|---|---|
| Configure Automatic Update | Enabled<br>- Auto download and schedule the install<br>- Scheduled install date: Every Day<br>- Scheduled install time: 12:00 | Hier wird festgelegt, dass die Patches automatisch vom SUS geladen werden und wann die Installation gestartet wird. |
| Specify intranet Microsoft update service location | Enabled<br>- Intranet update service: Servername vom vorhergehenden Kapitel<br>- Intranet statistics server: Servername vom vorhergehenden Kapitel | Mit intranet statistics server wird ist derjenige IIS gemeint, bei welchem die aktuellen Client Status ins Log (Webserver) geschrieben werden. |
| Reschedule Automatic Updates scheduled installations | Enabled<br>- Wait after system startup: 5 min | Schlägt ein Update fehl oder wird dieses vom Benutzer unterbrochen, wird der Update 5 min nach dem nächsten Reboot ausgeführt. |
| No auto-restart for scheduled Automatic Updates installations | Enabled | Hiermit wird der Benutzer informiert, dass neue Patches eingespielt wurden und der Computer neu gestartet werden muss. Es erfolgt kein automatischen Reboot! |

### 7.5.3 Update-Vorgang

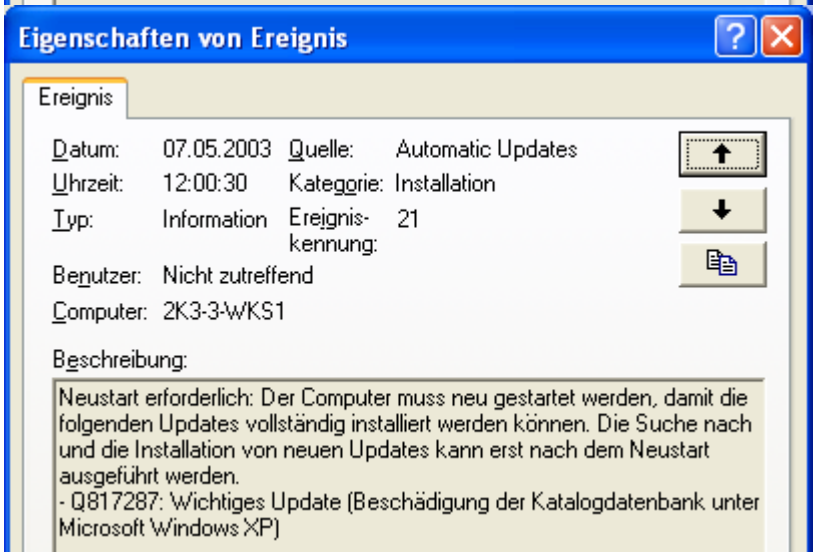
1. Der SUS lädt automatisch die Patches vom Microsoft Server herunter.
2. Ein Administrator überprüft und testet die Patches
3. Die Patches werden auf dem SUS Server freigegeben (approved)



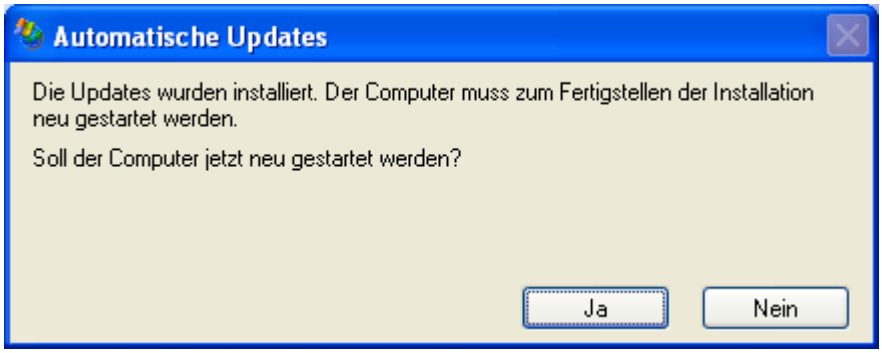

4. Die SUS-Clients laden innerhalb der nächsten 24h die neuen Patches herunter




5. Am darauf folgenden Mittag (12:00) werden die Patches auf den SUS-Clients installiert

6. Dem Benutzer wird folgender Dialog angezeigt.




7. Im Logfile (C:\WINDOWS\system32\LogFiles\W3SVC1) des IIS (SUS) wurden folgende Einträge gemacht:

```
2003-05-07 10:00:00 192.168.100.69 GET /wutrack.bin
V=1&U=e55841af69afae47961953fdcfcbd7a6&C=iu&A=n&I=&D=&P=5.1.a28.2.100.1.0&L=de-
DE&S=s&E=00000000&M=&X=030507095959656 80 - 192.168.100.92 Industry+Update+Control 200 0 0
2003-05-07 10:00:00 192.168.100.69 GET /wutrack.bin
V=1&U=e55841af69afae47961953fdcfcbd7a6&C=iu&A=n&I=&D=&P=5.1.a28.2.100.1.0&L=de-
DE&S=s&E=00000000&M=&X=030507100000047 80 - 192.168.100.92 Industry+Update+Control 200 0 0
```

### 7.5.4 Erzwingen des Updates

Damit man nicht 24h auf das Update eines SUS-Clients warten muss wird im Folgenden einen „Work-around“ beschrieben:

```
How to Force an Update Detection of the AutoUpdate Client
    Date - 08 Feb 2003
During normal operations, the Automatic Update client will check-in to the SUS Server every
17 to 22 hours to detect approved updates. It is possible to force the detection process.
Steps
1       Stop the "Automatic Updates" Service
2       Check that the "AUState" registry value, located at:
HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\
is set to "2"
3       Delete the "LastWaitTimeout" registry value, located at:
HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\
4       Start the "Automatic Updates" Service.
The Automatic Update client will begin the update detection process in approximately 10
minutes.
If an admin-priv user is logged on they will be presented with the option to install any
updates that downloaded, otherwise the computer will wait for the next scheduled install
time.
```

Quelle: http://www.susserver.com/Articles/AU-AutoUpdateCycle.asp

## 7.6 NT 4 Compliance

Folgende Einstellung wurden bezüglich der Rückwärtskompatibilität „aufgeweicht“. Es wird empfohlen diese zu bereinigen sobald keine NT4 Computer benutzt werden.

| # | Referenz | Parameter | Einstellung ohne NT4 |
|---|---|---|---|
| 1 | Hardening Domain #4203 | Network access: Allow anonymous SID/Name translation | Disabled<br><br>Falls diese Funktion abgeschaltet wird, wird die Funktion von RAS, SQL und Exchange Servern auf NT4.0 eingeschränkt! |
| 2 | Hardening Member Server #5517 | Domain member: Digitally encrypt or sign secure channel data (always) | Enabled<br><br>Dies kann nur eingeschaltet werden, wenn min. NT4 SP6a eingesetzt wird. |
| 3 | Hardening Member Server #5533 | Microsoft network client: Digitally sign communications (always) | Enabled |
| 4 | Hardening Member Server #5537 | Microsoft network server: Digitally sign communications (always) | Enabled |
| 5 | Hardening Member Server #5553 | Network security: LAN Manager authentication level<br>Send NTLMv2 response only\refuse LM & NTLM | Achtung beim Einsatz von Routing and Remote Access Server. Da muss diese Einstellung auf …\refuse LM zurückgestuft werden. |
| 6 | Hardening Member Server #5555 | Network security: Minimum session security for NTLM SSP based (including secure RPC) clients<br>No Minimum | Alle Einstellungen eingeschaltet |
| 7 | Hardening Member Server #5556 | Network security: Minimum session security for NTLM SSP based (including secure RPC) servers<br>No Minimum | Alle Einstellungen eingeschaltet |
| 8 | Hardening Domain Controller #6507 | Windows Internet Name Service (WINS) | Disabled |

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

## 7.7 Links

| Beschreibung | Link |
|---|---|
| The Threats and Countermeasures Guide contains detailed information about relevant security settings that can be configured on Microsoft Windows Server 2003 and Windows XP. | http://go.microsoft.com/fwlink/?LinkId=15159 |
| The Windows Server 2003 Security Guide provides levels of guidance for a number of server roles in multiple different client environments. This guidance includes steps to harden Domain Controllers, Infrastructure servers, File servers, Print servers, IIS servers, IAS servers, machines running Certificate Services, and bastion hosts. | http://go.microsoft.com/fwlink/?LinkId=14845 |
| System Services for the Windows Server 2003 Family and Windows XP Operating Systems | http://www.microsoft.com/technet/prodtechnol/windowsserver2003/plan/SvrXPSer.asp |
| Top Security Service Packs and Security Rollup Packs | http://www.microsoft.com/technet/security/tpsrvpck.asp |
| Feature Packs and Tools für Windows 2003 | http://www.microsoft.com/windowsserver2003/downloads/default.mspx |
| Download der Group Policy Management Console (GPMC) | http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=F39E9D60-7E41-4947-82F5-3330F37ADFEB |
| Group Policy Management Console (GPMC) | https://www.microsoft.com/windowsserver2003/gpmc/default.mspx |
| Microsoft Software Update Services (SUS) | http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp |
| SUSserver.com is a collection of Technical Information and Resources to assist in the implementation and troubleshooting of Microsoft Software Update Services. | http://www.susserver.com |
| SUS Server with SP1 Release Notes and Installation Instructions | http://www.microsoft.com/windows2000/windowsupdate/sus/sp1relnotes.asp |
| Windows Server 2003 Security Center | http://www.microsoft.com/technet/security/prodtech/windows/win2003/default.asp |
| Microsoft Security Notification Service | http://www.microsoft.com/security/security_bulletins/decision.asp |
| Microsoft Baseline Security Analyzer | http://www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp |
| Product Security Notification | http://www.microsoft.com/technet/security/bulletin/notify.asp |
| Vulnerability Scanner: Nessus | http://www.nessus.org |

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

| Beschreibung | Link |
|---|---|
| Netzwerk Scanner: LanGuard | http://www.gfi.com/lannetscan/ |
| Passwort Cracker: L0pht | http://www.atstake.com/research/lc/ |
| Passwort Cracker: Cain | http://www.oxid.it/cain.html |
| Google für Microsoft spezifische Webpages | http://www.google.com/microsoft |

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch