

# ***Empfehlungen zum Absichern von Windowssystemen***

*(Für Administratoren)*

Kein Betriebssystem ist sicher vor Angriffen, dies betrifft auch die verschiedenen Windows-Betriebssysteme. Obwohl sie mit der Zeit immer besser abgesichert und neu erkannte Sicherheitslücken geschlossen wurden, sind grundlegende Sicherheitsmaßnahmen erforderlich, um die Verwundbarkeit eines Betriebssystems zu minimieren.

Nähere Informationen bietet der englischsprachige Artikel "10 Immutable Laws of Security", der unter folgendem Link abgerufen werden kann:

[www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx](http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx).

## 1. Basisabsicherung von Windows-Betriebssystemen

### 1.1 Einrichten des Automatischen Windows-Update

Am einfachsten lässt sich ein Windows-Betriebssystem über Service Packs und Sicherheitsupdates von Microsoft auf dem Laufenden halten. Dazu wird auf einem Rechner das "automatische Windows Update" eingestellt und entsprechend konfiguriert. Dadurch wird sichergestellt, dass Schwachstellen im System zeitnah beseitigt werden.

Wie das "automatische Windows Update" aktiviert wird, ist auf den Web-Seiten des Rechenzentrums unter dem gleichnamigen Stichwort in der Rubrik "Rechenzentrum von A-Z" nachzulesen.

### 1.2 Update von Anwendungs-Software

Nicht nur das Betriebssystem ist Ziel von Hacker-Angriffen. Auch Anwendungs-Software weist Schwachstellen auf, die von böswilligen Angreifern ausgenutzt werden können. Anwendungs-Software sollte deshalb durch regelmäßige Updates auf dem neuesten Stand gehalten werden.

### 1.3 Nutzen des NTFS-Dateisystems, um die Sicherheitseinstellungen der Systempartition einzustellen

Eine weitere wichtige Sicherheitsmaßnahme ist die Nutzung des NTFS-Dateisystems. Nur dieses Dateisystem bietet Schutz vor unberechtigten Zugriffen auf gespeicherte Daten des PCs. Falls das veraltete FAT32-Dateisystem installiert ist, sollte es in ein NTFS-Dateisystem konvertiert werden.

Um die Sicherheitseinstellung auf einem Windows XP-System für die Systempartition C:/ zu ändern, sind beispielsweise die folgenden Arbeitsschritte durchzuführen:

Im Windows Explorer wird die Festplatte C:\ selektiert. Über den Menüpunkt "Datei -> Eigenschaften -> Sicherheit" sind die folgenden Sicherheitseinstellungen vorzunehmen:

Die Gruppe Jeder ist zu entfernen und durch Benutzer bzw. Authentifizierte Benutzer zu ersetzen. Das System braucht Vollzugriffsrechte.

Die Sicherheitseinstellungen der Systempartition (in der Regel liegt das Betriebssystem auf der Festplatte C:\) sollten auf die Parameter der unten aufgeführten Tabelle gesetzt werden.

Auszug aus den Sicherheitsempfehlungen der National Security Agency (USA) und Microsoft bezüglich der Absicherung einer Systempartition:

Administratoren	Vollzugriff	vererben
Ersteller-Besitzer	Vollzugriff nur für Unterordner und Dateien	
System	Vollzugriff	
Benutzer	Lesen, Ausführen	

(Quelle: <http://www.microsoft.com/technet/Security/topics/issues/w2kccscg/w2kscgc3.msp>)

**Hinweis:** Zugriffsrechte können nur vergeben werden, wenn als Dateisystem NTFS benutzt wird. Also unbedingt NTFS und nicht FAT/FAT32 benutzen!

## 1.4 Standardfreigaben entfernen

Üblicherweise besitzen alle Partitionen eines Rechners eine Standardfreigabe, die einen Namen in der Form "Laufwerksbuchstabe\$" (zum Beispiel: "C\$" für die erste Partition) hat. Diese Freigaben sind bekannt und können von Angreifern benutzt werden, um auf Rechner zuzugreifen. Deshalb sollten diese Freigaben gelöscht werden.

Dazu muss der folgende Eintrag in der Registrierungsdatei, dies geschieht mit dem Registrierungseditor regedit bzw. regedt32, vorgenommen werden.

**Hinweis:** Unter Windows XP ist regedt32 ein Link auf regedit.

HKEY\_LOCAL\_MACHINE/System/CurrentControlSet/Services/LanmanServer/Parameters  
DWORD-Wert AutoShareWks bzw. AutoShareServer erzeugen und auf 0 setzen

**Hinweis:** Das Arbeiten mit den Registrierungs-Tools sollte nur mit größter Sorgfalt erfolgen, da durch unsachgemäße Änderungen in der Registrierungsdatei das Betriebssystem Schaden nehmen kann.

## 1.5 Rechner in der Netzwerkumgebung verstecken

Damit ein Rechner nicht in der Netzwerkumgebung für andere sichtbar ist, kann er mit dem Befehl "net config server /hidden:yes" versteckt werden. Der Befehl ist in der Eingabeaufforderung (Start -> Programme -> Zubehör -> Eingabeaufforderung) auszuführen.

## 1.6 Aktivieren der Firewall

Um einen Rechner vor Angriffen von außen zu schützen, sollte eine Firewall installiert und aktiviert werden. Dabei sollten so wenig Ports auf einem Rechner offen sein wie unbedingt nötig.

Seit Windows XP ist im Betriebssystem eine Firewall integriert, die folgendermaßen aktiviert wird:

Auf einem Windows XP Rechner wird über Start -> Einstellungen -> Systemsteuerung -> Windows-Firewall und der Karteikarte Allgemein die Option Aktiv ausgewählt und mit OK bestätigt.

**Hinweis:** Damit Rechner für das Rechenzentrum über den "ping"-Befehl erreichbar sind, dies ist aus Supportgründen für das Rechenzentrum wesentlich, sollte die Firewall eingehende Echoanforderungen zulassen. Dies wird folgendermaßen in der Firewall eingetragen:

Über Start -> Einstellungen -> Systemsteuerung -> Windows-Firewall wird das gleichnamige Dialogfenster geöffnet. Auf der Karteikarte Erweitert ist im Abschnitt ICMP die Schaltfläche Einstellungen zu selektieren. Nun ist ein Häkchen im Optionsfeld "Eingehende Echoanforderungen zulassen" zu setzen. Der Dialog wird mit OK bestätigt.

## **1.7 Installieren eines Antivirenprogramms**

Auf jedes Betriebssystem gehört ein aktuelles Antivirenprogramm. Das Rechenzentrum bietet Universitätsangehörigen kostenlos das Virenschutzprogramm Sophos an. Näheres dazu ist auf den Web-Seiten des Rechenzentrums (<http://www.rz.uni-osnabrueck.de>) unter der Rubrik Rechenzentrum von A-Z zu erfahren.

## **1.8 Anti-Spyware Programme**

Es empfiehlt sich den Windows Defender zum Schutz vor Spyware zu installieren. Das Microsoft Programm ist kostenfrei und kann unter dem folgenden Link heruntergeladen werden:

<http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=435bfce7-da2b-4a6a-afa4-f7f14e605a0d>

Das Programm ist in verschiedenen Sprachen erhältlich und ist für Windows Server 2003 ab Service Pack 1 und Windows XP ab Service Pack 2 einsetzbar.

**Hinweis:** In Windows Vista ist dieses Programm Bestandteil des Betriebssystems.

## **1.9 Arbeiten mit eingeschränkten Benutzerrechten**

Die Administratorkennung sollte nur für Aufgaben, die ohne Administratorrechte nicht auszuführen sind, genutzt werden. Ansonsten sollte immer unter einem Benutzerkonto gearbeitet werden, dass nur über eingeschränkte Rechte auf dem Computer verfügt.

So wird der Rechner besser vor unerwünschtem Einschleusen und Ausführen von Schadprogrammen durch das Surfen im Internet geschützt.

## 1.10 Nutzen von starken Kennwörtern

Benutzerkennungen sollten generell mit einem möglichst komplizierten und nicht leicht zu erratenden Passwort bzw. Kennwort versehen werden. Empfohlene Richtlinien für Passwörter sind hierbei:

- mindestens acht Zeichen lang sein
- eine Kombination aus Buchstaben, Ziffern und Sonderzeichen

**Hinweis:** Standardmäßig hat das Administrator-Konto kein Passwort. Dies ist ein Sicherheitsloch, aber nur für die lokale Anmeldung. Ein Zugriff auf den Rechner von außen wird aber bei einer Benutzerkennung ohne Passwort unterbunden.

Eine Ausnahme stellt die Benutzerkennung "Gast" dar. Über diese Kennung kann, falls sie kein Passwort besitzt und nicht deaktiviert wurde, ein Zugriff auf einen Rechner stattfinden.

Informationen zu leeren Passwörtern und den Ausnahmen bzgl. des Gast-Accounts beim Zugriff auf Freigaben finden sich im Knowledgebase Artikel KB103390 mit dem Titel "Netzwerkzugriffsüberprüfungsalgorithmen und Beispiele für Windows Server 2003, Windows XP und Windows 2000" von Microsoft

(<http://support.microsoft.com/kb/103390>)

Mehr Informationen zu den empfohlenen Basissicherheitseinstellungen von Windows finden sich auf folgender Seite des Rechenzentrums der Universität Göttingen:

[http://www.gwdg.de/forschung/veranstaltungen/workshops/security\\_ws\\_2003/basissicherheit/smassnahmen\\_windows.pdf](http://www.gwdg.de/forschung/veranstaltungen/workshops/security_ws_2003/basissicherheit/smassnahmen_windows.pdf)

## 2. Richtlinien (Policies) zum Absichern von Windows Systemen

Richtlinien lassen sich mit dem Richtlinienditor `gpedit.msc` setzen. Der Richtlinienditor ist unter folgenden Windows-Versionen verfügbar: Windows 2000, Windows XP Professional, Windows Vista Business, Windows Vista Ultimate und Windows Vista Enterprise.

Die Home-Versionen von Windows XP und Windows Vista haben keinen Richtlinienditor.

Es lassen sich Richtlinien für Computer und Benutzer definieren. Über das Programm `gpedit.msc` lassen sich benutzerspezifische Richtlinien setzen, die für alle Benutzer gelten. Benutzer, die davon ausgenommen werden sollen, muss der lesende und der ausführende Zugriff auf die Datei `Registy.pol` im Verzeichnis `%windir%\system32\GroupPolicy\User` verweigert werden.

Alternativ lassen sich Richtlinien auch über den Registrierungseditor `regedit` bzw. `regedt32` setzen. Allerdings ist hier äußerste Sorgfalt angebracht, da falsche Einträge in der Registry zu einem instabilen oder unbrauchbaren System führen können.

Mögliche Registry-Einträge lassen sich aus einer Excel-Datei von Microsoft, in der die zu den Richtlinien gehörenden Registrierungseinträge vermerkt sind, entnehmen.

Diese Excel-Datei mit Namen `VistaGPSettings.xls` ist im Downloadbereich von Microsoft unter dem Stichwort "Group Policy Settings Reference Windows Vista" zu finden. Sie enthält neben den Registrierungseinträgen für Vista, die möglichen Einträge für andere Windows-Betriebssysteme.

Zum Zeitpunkt des Verfassens dieser Hinweise war die Datei auf der folgenden Web-Seite verfügbar:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=41dc179b-3328-4350-ade1-c0d9289f09ef&DisplayLang=en>

**Hinweis:** Unter Windows XP Professional lassen sich benutzerspezifische Richtlinien "auch" speziellen Benutzern oder Gruppen zuordnen. "Allerdings" benötigt man dazu das Programm Poledit aus dem Resource Kit für Office XP. Dieser Policy-Editor verfügt über die gleichen Möglichkeiten wie der gleichnamige Policy-Editor unter Windows NT. Um Richtlinien festzusetzen, müssen spezielle "adm-Dateien" (Vorlagendateien) vorhanden sein.

Das Resource Kit für Office XP ist über sie folgende Web-Seite erhältlich:

<http://www.microsoft.com/office/orkarchive/XPddl.htm>

Hier finden sich auch Verweise zur Nutzung und zur Erstellung von adm-Dateien.

Muster Vorlagen bzw. adm-Dateien sind ebenfalls auf

<http://www.gruppenrichtlinien.de/index.html?/info/Downloads.htm> verfügbar.

Unter Windows Vista gibt es die Möglichkeit für bestimmte Benutzer oder Gruppen gezielt Policies einzustellen. Hier lassen sich über die Managementkonsole (mmc.exe) "Multiple Local Group Policy" definieren. Das englischsprachige Dokument von Microsoft "Windows Vista: Step-by-Step Guide to Managing Multiple Local Group Policy" vom August 2006 beschreibt wie es geht.

siehe:

<http://technet2.microsoft.com/WindowsVista/en/library/9c7ecc7d-8784-4b8d-ba1f-ba1882ba83741033.mspx?mfr=true>

oder als Word-Datei unter:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=311f4be8-9983-4ab0-9685-f1bfec1e7d62&DisplayLang=en>

## 2.1 Überwachungsrichtlinien

Überwachungsrichtlinien helfen, die genauen Umstände von Sicherheitsverletzungen zu bestimmen. Es sollten erfolgreiche Aktionen, wie Anmeldeversuche und Anmeldeereignisse, Veränderungen von Richtlinieneinstellungen und Systemereignisse überwacht werden.

Die Überwachungsrichtlinien finden sich nach dem Starten des Programms gpedit.msc unter:

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Überwachungsrichtlinie in der linken Fensterhälfte.

**Hinweis:** Alles, was sich unterhalb des Baumes Sicherheitseinstellungen konfigurieren lässt, kann auch mit dem Tool secpol.msc bearbeitet werden.

Richtlinie	Einstellung
Anmeldeversuche überwachen	Erfolg
Kontenverwaltung überwachen	Erfolg
Anmeldeereignisse überwachen	Erfolg
Richtlinienänderungen überwachen	Erfolg
Systemereignisse überwachen	Erfolg

**Hinweis:** Die NSA empfiehlt eine zusätzliche Überwachung der Ereignisse im Fall eines Fehlers.

## 2.2 Zuweisen von Benutzerrechten

Durch Zuweisen von Benutzerrechten lässt sich steuern, wer mit welchen Privilegien Zugriff auf einen Computer und seine Ressourcen hat. Hierzu werden einzelnen Richtlinien individuelle Benutzer bzw. Gruppen zugewiesen.

Um den Wert eines Benutzerrechtes auf **Niemand** zu setzen, aktiviert man die Einstellung, fügt jedoch **keinen** Benutzer bzw. keine Gruppe hinzu. Um den Wert eines Benutzerrechtes auf **Nicht definiert** zu setzen, wird die Einstellung nicht aktiviert.

Die Einstellungen zum Zuweisen von Benutzerrechten befinden sich im Programm **gpedit.msc** unter:

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\  
Lokale Richtlinien\Zuweisen von Benutzerrechten

Richtlinie - Benutzerrechte	Einstellung
Auf diesen Computer vom Netzwerk aus zugreifen	Administratoren
Einsetzen als Teil des Betriebssystems	Niemand
Anpassen von Speicherkontingenten für einen Prozess	Administratoren, Lokaler Dienst, Netzwerkdienst
Lokal anmelden zulassen	Benutzer, Administratoren
Anmeldung über Terminaldienste zulassen	
Falls Remotedesktop-Zugriff erforderlich ist, Administratoren statt Niemand eintragen	Niemand
Sichern von Dateien und Verzeichnissen	Administratoren
Auslassen der durchsuchenden Prüfung	Administratoren, Benutzer
Ändern der Systemzeit	Administratoren
Auslagerungsdatei erstellen	Administratoren
Permanente freigegebene Objekte erstellen	Niemand
Erstellen eines Tokenobjekts	Niemand
Debuggen von Programmen	Niemand
Den Zugriff auf diesen Computer vom Netzwerk aus verweigern	Support_388945a0, Gast
Anmeldung als Batchauftrag verweigern	Support_388945a0, Gast
Lokal anmelden verweigern	Support_388945a0, Gast, beliebige Dienstkonto
Anmeldung über Terminaldienste verweigern	
Falls Remotedesktopverbindungen z. B. für Administratoren zugelassen sein sollen, muss Benutzer statt Jeder eingetragen werden.	Jeder
Computer und Benutzerkonten für Delegierungszwecke vertrauen	Niemand
Erzwingen des Herunterfahrens von einem Remotesystem aus	Administratoren

Richtlinie - Benutzerrechte	Einstellung
Generieren von Sicherheitsüberwachungen	Lokaler Dienst, Netzwerkdienst
Anheben der Zeitplanungspriorität	Administratoren
Laden und Entfernen von Gerätetreibern	Administratoren
Seiten im Speicher sperren	Niemand
Anmelden als Stapelverarbeitungsauftrag	Niemand
Als Dienst anmelden	Netzwerkdienst, lokaler Dienst
Verwalten von Überwachungs- und Sicherheitsprotokoll	Administratoren
Firmware-Umgebungsvariablen ändern	Administratoren
Wartungsaufgaben für Speichermedien ausführen	Administratoren
Einzelprozessprofil erstellen	Administratoren
Erstellen eines Profils der Systemleistung	Administratoren
Entfernen eines Computers aus der Dockingstation	Administratoren, Benutzer
Ersetzen eines Prozessebenentokens	Lokaler Dienst, Netzwerkdienst
Wiederherstellen von Dateien und Verzeichnissen	Administratoren
System herunterfahren	Administratoren, Benutzer
Übernehmen des Besitzes an Dateien und Objekten	Administratoren

Nähere Erläuterungen zu den einzelnen Richtlinien finden sich im Kapitel 3 des Sicherheitshandbuchs für Windows XP

([http://www.microsoft.com/germany/technet/sicherheit/prodtech/windowsxp/secwinxp/xpsgc\\_h03.mspix](http://www.microsoft.com/germany/technet/sicherheit/prodtech/windowsxp/secwinxp/xpsgc_h03.mspix))

### 2.3 Einstellungen der Sicherheitsoptionen

Die Einstellungen für Sicherheitsoptionen können für die Aktivierung und Deaktivierung von Berechtigungen und Funktionen (wie z. B. des Zugriffs auf Disketten- und CD-ROM-Laufwerke sowie der Anmeldeaufforderung) benutzt werden. Diese Einstellungen werden auch zum Konfigurieren verschiedener anderer Einstellungen verwendet, wie z. B. zur digitalen Datensignierung oder für die Funktionsweise der Treiberinstallation. Ebenfalls festgelegt werden hier die Sicherheitseinstellungen für Netzwerkzugriffe

Alle Richtlinien finden sich im Programm `gpedit.msc` unter:

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen

Richtlinie - Konten	Einstellung
Konten: Administratorkonto umbenennen	Empfohlen
Konten: Administratorkontostatus	Aktiviert
Konten: Gastkontenstatus	Deaktiviert
Konten: Gastkonto umbenennen	Empfohlen

<b>Richtlinie - Konten</b>	<b>Einstellung</b>
Konten: Lokale Kontenverwendung von leeren Kennwörtern auf Konsolenanmeldung beschränken	Aktiviert

<b>Richtlinie - Überwachung</b>	<b>Einstellung</b>
Überwachung: Die Verwendung des Sicherungs- und Wiederherstellungsrechts überprüfen	Deaktiviert
Überwachung: System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können	Deaktiviert
Überwachung: Zugriff auf globale Systemobjekte prüfen	Deaktiviert

<b>Richtlinie - Geräte</b>	<b>Einstellung</b>
Geräte: Anwendern das Installieren von Druckertreibern nicht erlauben	Aktiviert
Geräte: Entfernen ohne vorherige Anmeldung erlauben	Deaktiviert
Geräte: Formatieren und Auswerfen von Wechselmedien zulassen	Administratoren
Geräte: Verhalten bei der Installation von nicht signierten Treibern	Warnen, aber Installation erlauben
Geräte: Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken	Aktiviert
Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken	Aktiviert

<b>Richtlinie – Interaktive Anmeldung</b>	<b>Einstellung</b>
Interaktive Anmeldung: Anwender vor Ablauf des Kennworts zum Ändern des Kennworts auffordern	14 Tage
Interaktive Anmeldung: Anzahl zwischenspeichernder vorheriger Anmeldungen (für den Fall, dass der Domänencontroller nicht verfügbar ist)	0
Interaktive Anmeldung: Domänencontrollerauthentifizierung zum Aufheben der Sperrung der Arbeitsstation erforderlich	Aktiviert
Interaktive Anmeldung: Kein STRG+ALT+ENTF erforderlich	Deaktiviert
Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen	Aktiviert
Interaktive Anmeldung: Nachricht für Benutzer, die sich anmelden möchten	

<b>Richtlinie – Interaktive Anmeldung</b>	<b>Einstellung</b>
Interaktive Anmeldung: Nachrichtentitel für Benutzer, die sich anmelden möchten	
Interaktive Anmeldung: Verhalten beim Entfernen von Smartcards	Nicht definiert

<b>Richtlinie – Microsoft-Netzwerk</b>	<b>Einstellung</b>
Microsoft-Netzwerk (Client): Kommunikation digital signieren (immer) (in Zusammenhang mit unserem Samba-Fileserver)	Deaktiviert
Microsoft-Netzwerk (Client): Kommunikation digital signieren (wenn Server zustimmt)	Aktiviert
Microsoft-Netzwerk (Client): Unverschlüsseltes Kennwort an SMB-Server von Drittanbietern senden	Deaktiviert
Microsoft-Netzwerk (Server): Leerlaufzeitspanne bis zum Anhalten der Sitzung	99999
Microsoft-Netzwerk (Server): Kommunikation digital signieren (immer) (in Zusammenhang mit unserem Samba-Server)	Deaktiviert
Microsoft-Netzwerk (Server): Kommunikation digital signieren (wenn Client zustimmt)	Aktiviert

<b>Richtlinie - Netzwerkzugriff</b>	<b>Einstellung</b>
Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten nicht erlauben	Aktiviert
Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten nicht erlauben	Aktiviert
Netzwerkzugriff: Anonyme SID-/Namensübersetzung zulassen	Deaktiviert
Netzwerkzugriff: Die Verwendung von 'Jeder'-Berechtigungen für anonyme Benutzer ermöglichen	Deaktiviert
Netzwerkzugriff: Freigaben, auf die anonym zugegriffen werden kann	comcfg, dfs\$
Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten	Klassisch – lokale Benutzer authentifizieren sich als sie selbst
Netzwerkzugriff: Named Pipes, auf die anonym zugegriffen werden kann	* In der folgenden Einstellungsbeschreibung finden Sie eine vollständige Liste von Named Pipes
Netzwerkzugriff: Registrierungspfade, auf die von anderen Computern aus zugegriffen werden kann	* In der folgenden Einstellungsbeschreibung finden Sie eine vollständige Liste von Pfaden
Netzwerkzugriff: Speicherung von Anmeldeinformationen oder .NET-Passports für die Netzwerkauthentifikation nicht erlauben	Aktiviert

<b>Richtlinie - Netzwerksicherheit</b>	<b>Einstellung</b>
Netzwerksicherheit: Keine LAN Manager-Hashwerte für nächste Kennwortänderung speichern	Aktiviert
Netzwerksicherheit: LAN Manager-Authentifizierungsebene	Nur NTLMv2-Antworten senden\LM und NTLM verweigern
Netzwerksicherheit: Minimale Sitzungssicherheit für NTLM-SSP-basierte Clients (einschließlich sicherer RPC-Clients)	Nachrichtervertraulichkeit erfordern, Nachrichtenintegrität erfordern, NTLMv2-Sitzungssicherheit erfordern, 128-Bit-Verschlüsselung erfordern
Netzwerksicherheit: Minimale Sitzungssicherheit für NTLM-SSP-basierte Server (einschließlich sicherer RPC-Server)	Nachrichtervertraulichkeit erfordern, Nachrichtenintegrität erfordern, NTLMv2-Sitzungssicherheit erfordern, 128-Bit-Verschlüsselung erfordern
Netzwerksicherheit: Signaturanforderungen für LDAP-Clients	Signatur aushandeln

Durch die folgende Richtlinieneinstellung wird festgelegt, welche Kommunikationssitzungen oder Pipes über Attribute und Berechtigungen verfügen, die anonymen Zugriff zulassen.

<b>Richtlinie - Netzwerkzugriff</b>	<b>Einstellung</b>
Netzwerkzugriff: Named Pipes, auf die anonym zugegriffen werden kann	COMNAP,COMNODE,SQL\QUERY,SPOOLSS,LLSRPC,Browser

Durch die folgende Richtlinieneinstellung wird festgelegt, auf welche Registrierungspfade zugegriffen werden kann, nachdem der Schlüssel WinReg zur Feststellung der Zugriffsberechtigungen für diese Pfade ausgewertet wurde.

<b>Richtlinie - Netzwerkzugriff</b>	<b>Einstellung</b>
Netzwerkzugriff: Registrierungspfade, auf die von anderen Computern aus zugegriffen werden kann	System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Control\Server Applications, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, Software\Microsoft\Windows NT\CurrentVersion

### 3. Remote-Zugriff auf die Registrierungsdatei einschränken oder unterbinden

Es wird dringend empfohlen, den Zugriff auf die eigene Registrierungsdatei von anderen Rechnern aus nur ausgewählten Benutzern zu erlauben oder sogar komplett zu verbieten.

**Hinweis:** Standardmäßig ist der Remote-Zugriff erlaubt!

Viele Viren benutzen diese Sicherheitslücke, und setzen beispielsweise im Registrierungsschlüssel „Run“ einen neuen Eintrag, über den schadhafte Programme beim Starten des Rechners ausgeführt werden.

#### 3.1 Remote-Zugriff auf die Registrierungsdatei ausgewählten Benutzern erlauben

Der folgende Eintrag kann unter Zuhilfenahme des Systemprogramms „regedt32“ gesetzt werden. (Start -> Ausführen -> "regedt32" -> OK )

HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\WINREG

Unter dem Menüpunkt Bearbeiten -> Berechtigungen können ausgewählte Benutzer eingetragen werden, die berechtigt sind auf die Registrierungsdatei zuzugreifen.

#### 3.2 Remote-Zugriff auf die Registrierungsdatei verbieten

Der Zugriff von außen auf die Registrierungsdatei wird unterbunden durch die Deaktivierung des "Remote-Registrierungsdienstes" im Menü Start -> Einstellungen -> Systemsteuerung -> Verwaltung -> Dienste

### 4. Internet Explorer

In Kapitel 4 des deutschen Windows XP Sicherheitshandbuchs von Microsoft wird eine ganze Reihe von Vorschlägen zum Absichern des Internet Explorers gemacht. Insbesondere sollte man darüber nachdenken, die Installation von Internet Explorer-Komponenten, von Add-Ons und ActiveX-Steurelementen einzuschränken. Auch das Verändern der Sicherheitszonen und das Umgehen mit MIME-Daten sind zu beachten, genauso wie der Dateidownload.

An dieser Stelle ist es nicht möglich alle Sicherheitseinstellungen zu besprechen. Es empfiehlt sich die von Microsoft zur Verfügung gestellten Security Guides zu lesen. Ebenfalls interessant sind die Empfehlungen des Heise Verlages über den c't Browsercheck des Internet Explorer 7 (<http://www.heise.de/security/dienste/browsercheck/anpassen/ie70>).

### 5. Windows Explorer

Ein sicheres Windowssystem erfordert einige Einstellungen für den Windows Explorer, die sich unter Extras > Ordneroptionen > Ansicht durchführen lassen.

Hier einige grundlegende Empfehlungen:

1. „Automatisch nach Netzwerkordnern und Druckern suchen“ **deaktivieren**
  - falls aktiviert, kann es in großen Netzen zu zuviel Last führen
  - falls aktiviert, werden viele Anmeldeversuche vom System durchgeführt und es kann eventuell zu einer Übertragung des Benutzernamens/Kennworts kommen

- besonders kritisch ist, das es hierbei zu Übertragung von Kennwörtern im Klartext kommen kann (falls eingestellt)
- 2. „Einfache Dateifreigabe verwenden (empfohlen)“ **deaktivieren**
  - wird benötigt um Dateisystemrechte über die graphische Oberfläche (Registerkarte "Sicherheit") einzustellen
  - sollte bei Benutzern, die keine Admin-Rechte haben aktiviert bleiben.
- 3. „Erweiterungen bei bekannten Dateitypen ausblenden“ **deaktivieren**
  - so lassen sich Dateitypen erkennen. Dies ist wichtig, um Dateien, die als Anhänge per E-Mail gesendet werden, zu identifizieren. Wird der Dateityp nicht angezeigt, können Viren-verseuchte E-Mails falsche Dateien vortäuschen und so den Rechner infizieren. (so wird zum Beispiel bei aktivierter Direktive aus der Datei "Wurm.txt.vbs" optisch die Datei "wurm.txt")
- 4. „Ordnerfenster im eigenen Prozess starten“ **aktivieren**
  - um ein privilegiertes Fenster mit „Ausführen als“ zu erzeugen.

Administratoren sollten zusätzlich folgende Direktiven setzen:

- „Geschützte Systemdateien ausblenden (empfohlen)“ **deaktivieren**,
- "Inhalte von Systemordnern anzeigen" **aktivieren**,
- „Versteckte Dateien und Ordner“ > „Alle Dateien und Ordner anzeigen“ **aktivieren**

(vgl. Basissicherheitsmaßnahmen bei Windows-Systemen, GWDG)

## 6. E-Mail-Nutzung

Es ist nicht unerheblich, welcher E-Mail-Klient zum Lesen, Schreiben und Versenden von E-Mails benutzt wird. Ein beliebtes Ziel für Hacker sind E-Mail Programme. Es sollte darauf geachtet werden, dass nur aktuelle Programmversionen benutzt werden. Generell empfiehlt es sich keine Attachements zu öffnen, die von unbekanntem Absendern kommen. Außerdem sollten Mails nur als "reiner Text" angezeigt werden. So wird das Ausführen von verstecktem Code in E-Mails verhindert.

Das Rechenzentrum setzt auf Rechnern im PC-Pool des AVZs das Programm Thunderbird ein.

**Hinweis:** Aus Sicherheitsgründen sollte beim Einsatz von Thunderbird Java-Script für E-Mail und Diskussionsgruppen deaktiviert sein!

## 7. Weitere Sicherheitsmaßnahmen

1. Ausführlicher Beschreibungen verschiedener Sicherheitsmaßnahmen finden sich auf den Web-Seiten von Microsoft.  
<http://www.microsoft.com/downloads/Search.aspx?displaylang=en>  
 Hier sucht man unter Angabe von Windows Security & Updates in der ersten Spalte und Security Guide in der zweiten Spalte nach entsprechender Literatur zum Download. Zurzeit (Stand 29.05.2008) werden dort u. a. englischsprachige Sicherheitsrichtlinien zu
  - Windows 2000
  - Windows XP
  - Windows Vista

- Windows Server 2003
- Windows Server 2008

angeboten.

2. Über die Security Guidance Seite von Microsoft Technet: (<http://www.microsoft.com/technet/security/guidance/default.aspx>) erhält man weitere Skripte zu Sicherheitseinstellungen, u. a. auch zum Windows 2000 Server. Deutschsprachige Literatur von Microsoft, ist meist nicht so aktuell wie die englischsprachigen Dokumente, erhält man auf folgender Seite: <http://www.microsoft.com/germany/technet/sicherheit/default.aspx>  
Hier sind die Sicherheitshandbücher zu empfehlen.  
In Kapitel 3 des Sicherheitshandbuches für Windows XP werden u. a. Empfehlungen für Einstellungen zum Zuweisen von Benutzerrechten und Empfehlungen für die Einstellungen der Sicherheitsoptionen gegeben. Im Anhang A des deutschsprachigen Sicherheitshandbuches zu Windows XP werden wichtige Hinweise zu Einstellungen des Internet Explorers, des Remoteprozeduraufrufs, der Windows Firewall und des Anlagenmanagers gegeben.
3. Weitere Sicherheitshandbücher bietet die NSA (National Security Agency) der Vereinigten Staaten von Amerika an: [http://www.nsa.gov/snac/downloads\\_winvista.cfm?MenuID=scg10.3.1.1](http://www.nsa.gov/snac/downloads_winvista.cfm?MenuID=scg10.3.1.1)  
Hier finden sich neben Empfehlungen für die Windows-Betriebssysteme auch Sicherheitsempfehlungen für MAC OS und Linux-Systeme (SUN Solaris und Red Hat Enterprise).

Grundsätzliche Erwägungen und Empfehlungen gibt auch der Leitfaden IT-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik:

<http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf>

*Tabellarische Übersicht weiterführender Links:*

Basissicherheitsmaßnahmen bei Windows-Systemen	<a href="http://www.gwdg.de/forschung/veranstaltungen/workshops/security_ws_2003/basissicherheitsmassnahmen_windows.pdf">http://www.gwdg.de/forschung/veranstaltungen/workshops/security_ws_2003/basissicherheitsmassnahmen_windows.pdf</a>
TechNet Security Center	<a href="http://technet.microsoft.com/de-de/security/default(en-us).aspx">http://technet.microsoft.com/de-de/security/default(en-us).aspx</a>
Microsoft Security at home (Windows Vista)	<a href="http://www.microsoft.com/protect/default.aspx">http://www.microsoft.com/protect/default.aspx</a>
Microsoft Windows XP Security Guide	<a href="http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.aspx">http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.aspx</a>
Step-by-Step Guide to Securing Windows XP Professional with Service Pack 2 in Small and Medium Businesses	<a href="http://download.microsoft.com/download/9/4/d/94dd17e2-1a63-4094-a560-e15bff312dfc/XPSP2SMB.pdf">http://download.microsoft.com/download/9/4/d/94dd17e2-1a63-4094-a560-e15bff312dfc/XPSP2SMB.pdf</a>
Sicherheitseinstellungen unter Windows Server 2003 und Windows XP	<a href="http://www.microsoft.com/germany/technet/sicherheit/topics/serversecurity/tcg/tcgch01n.aspx">http://www.microsoft.com/germany/technet/sicherheit/topics/serversecurity/tcg/tcgch01n.aspx</a>
Windows, aber sicher (c't 5/2007, S. 128 Windows-Sicherheit)	<a href="http://www.heise.de/ct/07/05/128/default.shtml">http://www.heise.de/ct/07/05/128/default.shtml</a>
National Security Agency - Operating Systems Guides	<a href="http://www.nsa.gov/snac/downloads_winvista.cfm?MenuID=scg10.3.1.1">http://www.nsa.gov/snac/downloads_winvista.cfm?MenuID=scg10.3.1.1</a>
Security Guidance for Windows XP	<a href="http://www.microsoft.com/technet/security/prodtech/windowsxp.aspx">http://www.microsoft.com/technet/security/prodtech/windowsxp.aspx</a>

TechNet Sicherheit – Sicherheitsportal für IT-Profis	<a href="http://www.microsoft.com/germany/technet/sicherheit/default.aspx">http://www.microsoft.com/germany/technet/sicherheit/default.aspx</a>
Windows Vista richtig absichern	<a href="http://www.inet-forum.de/index.php?page=Thread&amp;threadID=288">http://www.inet-forum.de/index.php?page=Thread&amp;threadID=288</a>
c't-Browsercheck: Sicherheitseinstellungen des Internet Explorer 7 anpassen	<a href="http://www.heise.de/security/dienste/browsercheck/anpassen/ie70">http://www.heise.de/security/dienste/browsercheck/anpassen/ie70</a>