Bundesamt für Sicherheit in der Informationstechnik

Revisionskonzept zu Windows NT

Basierend auf dem IT-Grundschutzhandbuch

Version 1.01

Versionsdatum: 22.09.1999

Ansprechpartner: BSI, Referat VI 3, Thomas Biere
E-Mail: gshb@bsi.de

Zielsetzung

Die vorliegende Checkliste stellt ein ergänzendes Hilfsmittel zum IT-Grundschutzhandbuch des BSI dar. Sie soll als Werkzeug dazu dienen, mit möglichst geringem Zeitaufwand festzustellen, welche der notwendigen IT-Sicherheitsmaßnahmen in einem zu untersuchenden Windows NT-System umgesetzt sind. Inhaltlich beschränkt sich die Checkliste dabei auf Kapitel 6.4 „Windows NT Netz" des IT-Grundschutzhandbuchs.

Da sich die Informationstechnik in einem ständigen Wandel befindet, ist es in der Regel nicht ausreichend, zu einem bestimmten Zeitpunkt eine IT-Grundschutz-Untersuchung durchzuführen, ein entsprechendes Sicherheitskonzept zu erarbeiten und die nach einem Soll/Ist-Vergleich als notwendig erkannten Maßnahmen umzusetzen. Zudem sind oft viele Personen am IT-Sicherheitsprozess beteiligt, z. B. die Leitung der Organisation, das IT-Sicherheitsmanagement, die Administratoren und auch die Benutzer selbst. Notwendig ist daher eine kontinuierliche Kontrolle der Wirksamkeit des IT-Sicherheitskonzeptes, der Aktualität der umgesetzten Maßnahmen und auch der Qualität der Aufgabenwahrnehmung, z. B. der Administration eines Servers oder des Umgangs mit Passwörtern. Die hier vorgestellte Checkliste kann bei der Erstellung eines geeigneten Revisionskonzeptes mit einfließen.

Um eine praxis- und bedarfsgerechte Weiterentwicklung und Aktualisierung dieser Checkliste zu erreichen, benötigt das BSI Ihre Mithilfe. Kommentare, Kritik, Verbesserungsvorschläge, Anregungen und Ergänzungen sind daher in ganz besonderem Maße willkommen und werden erbeten an folgende E-Mail-Adresse: *gshb@bsi.de* .

Vorkenntnisse

Die Anwendung der Checkliste setzt Kenntnisse in den Bereichen Administration von Windows NT und Hardware-Komponenten von Server- bzw. Client-Computern voraus. Ein potentieller Anwender sollte in der Lage sein, mit den von Windows NT mitgelieferten Administrations- und Konfigurations-Werkzeugen (z. B. Benutzermanager für Domänen) die gewünschten Informationen zu ermitteln.

Die Checkliste soll und kann kein Wissen zu der zugrundeliegenden Sicherheitsproblematik vermitteln. Dies ist u. a. Aufgabe des IT-Grundschutzhandbuchs. Daher wird in der Checkliste auf die entsprechenden Maßnahmen des IT-Grundschutzhandbuchs verwiesen.

Aufbau der Checkliste

Die Checkliste für Windows NT liegt als strukturierter Fragenkatalog vor. Die Fragen sind dabei nach thematischen bzw. logischen Gesichtspunkten gegliedert. Z. B. findet sich im Kapitel 500 „Benutzermanagement" der Bereich 530 „Benutzerrechte". Die Gliederung innerhalb der einzelnen Bereiche dient vor allem dazu, abhängig von der konkreten Konfiguration des vorliegenden IT-Systems die relevanten Fragen auszuwählen. Dies ist notwendig, da sich Windows NT-Installationen beispielsweise im Hinblick auf

- **installierte Hardware-Komponenten,**
- **installierte Dienste und Protokolle und**
- **Einsatzart (z. B. Domänencontroller oder dedizierter Server)**

erheblich unterscheiden können. Die Checkliste trägt diesen Unterschieden mit Hilfe von Fragestrukturen der folgenden Art Rechnung:

710.04	**Falls das untersuchte System mit einem CD-ROM-Laufwerk ausgestattet ist:**
710.04.1	**Frage 1**
	usw.
	Ende {Falls das untersuchte System mit einem CD-ROM-Laufwerk ausgestattet ist: }

Um eine einfache und formalisierte Auswertung zu ermöglichen, sind die meisten Fragen in der Checkliste Entscheidungsfragen, d. h. bei der Anwendung ist die Spalte „Ja“ bzw. „Nein“ zu markieren. Die Fragen sind dabei so formuliert, dass ein „Ja“ eine Konfiguration im Sinne des IT-Grundschutzhandbuchs bedeutet. Die Antwort „Nein“ dagegen weist auf eine potentielle Sicherheitslücke hin. Ausnahmen stellen dabei natürlich solche Fragen dar, mit denen festgestellt wird, ob nachfolgende Fragen relevant sind, z. B. die obige Frage nach dem Vorhandensein eines CD-ROM-Laufwerks.

Ein Teil der Fragen sind keine Entscheidungsfragen, sondern erfordern eine inhaltliche Antwort. Wichtige Beispiele sind Fragen nach verantwortlichen Personen und nach Prüfungsintervallen. Die hierbei erfassten Daten dienen teilweise als Grundlage für nachfolgende Fragen.

Vorgehensweise

Für die konkrete Anwendung der vorliegenden Checkliste gibt es unterschiedliche Ansätze. Zunächst ist es natürlich möglich, die Checkliste für jedes vorhandene Windows NT-System vollständig der Reihe nach abzuarbeiten. Aufgrund des Umfangs des Fragenkatalogs ist dies jedoch nur bei kleinen IT-Anlagen effektiv durchführbar. Stattdessen empfehlen wir die im folgenden beschriebene Vorgehensweise:

1. **Klassifizierung der zu untersuchenden Windows NT-Systeme**

   Insbesondere bei großen Client-Server-Systemen gibt es häufig eine große Zahl von Computern, bei denen sowohl die Hardware- als auch die Software-Konfiguration nahezu identisch ist. Teilweise wird dies sogar durch geeignete Management-Software erzwungen. In diesem Fall ist es sinnvoll, aus jeder Klasse von Computern eine kleine Anzahl auszuwählen und auf diese Computer die Checkliste anzuwenden.

2. **Identifizieren von übergeordneten Fragenbereichen**

   In der Checkliste befinden sich Fragen zum Domänenkonzept. Diese Fragen brauchen nicht bei jedem Windows NT-System abgearbeitet zu

werden. Stattdessen reicht es aus, dies für jede Domäne, ggf. auch nur einmal für die gesamte Organisation zu tun. Je nach Einsatzumfeld lassen sich ggf. weitere Bereiche aus dem Fragenkatalog isolieren, die systemübergreifend beantwortet werden können.

3. **Löschen der irrelevanten Fragenbereiche**

   Aus der Checkliste werden alle Fragenbereiche gelöscht, die für das betrachtete System (oder die betrachtete Klasse von Systemen) nicht relevant sind. Aufgrund der oben beschriebenen Struktur des Fragenkatalogs sind diese Bereiche leicht zu identifizieren.

4. **Abarbeiten der verbleibenden Fragen**

   Die verbleibenden Fragen werden anhand des vorliegenden Systems (oder der vorliegenden Klasse von Systemen) beantwortet. Bei den Entscheidungsfragen wird das Ergebnis in den Spalten „Ja“ bzw. „Nein“ und „Bemerkungen / Kommentare / Begründungen“ dokumentiert. Bei den übrigen Fragen kann es je nach Umfang notwendig sein, das Ergebnis in einem separaten Anhang zu erfassen und in der Checkliste auf diesen Anhang zu verweisen. Befragte Person ist in der Regel das Administrationspersonal. Eine Ausnahme stellt hier das Kapitel 160 „Benutzerorientierte Fragen“ dar.

Ergänzende Hinweise

Ist für das zu untersuchende IT-System ein Sicherheitskonzept nach dem IT-Grundschutzhandbuch erstellt worden und sind entsprechende Maßnahmen umgesetzt, so müssen die Fragen nicht auf einmal abgearbeitet werden. Vielmehr bietet es sich an, die Abarbeitung der Fragen mit Hilfe eines Prüfplans auf mehrere Jahre zu verteilen. Dadurch wird ein kontinuierlicher Prüfprozess gewährleistet.

Im Rahmen einer kontinuierlichen Revision lassen sich Prüfungen, die nach der vorliegenden Checkliste durchzuführen sind, in den administrativen Aufgabenbereich verlagern. Hierzu protokolliert der Administrator die Durchführung und das Ergebnis der von ihm regelmäßig getätigten Prüfungen. Die Revision kann sich dann darauf beschränken, die Prüfprotokolle zu sichten und Stichproben durchzuführen.

Inhaltsverzeichnis

100 Sicherheitspolicy

110 Sicherheitsstrategie

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
110.01	**Ist die Sicherheitsstrategie dokumentiert und den Benutzern im notwendigen Umfang bekannt gemacht worden?**				**M 2.91**
110.02	**Wird die Sicherheitsstrategie an Veränderungen im Einsatzumfeld angepasst?**				**M 2.91**
110.03	**Wer ist für die Überprüfung und Anpassung der Sicherheitsstrategie zuständig?**				**M 2.91**
110.04	**Wie lang ist ein Prüfungsintervall?**				**M 2.91**
110.05	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 2.91**
110.06	**Werden entsprechende Prüfungen und Anpassungen dokumentiert?**				**M 2.91**

Befragte Person: Geprüft von: Datum:

120 Notfallvorsorge

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
120.01	Ist für den betrachteten Rechner eine Notfalldis-kette vorhanden?				M 4.55 M 6.42
120.02	Sind für den betrachteten Rechner die Setup-Dis-ketten vorhanden?				M 4.55 M 6.42
120.03	Wo werden die zum System gehörenden Setup-Disketten, die Notfalldiskette und evtl. vorhandene Bandsicherungen auf-bewahrt?				M 4.77
120.04	Sind die zum System gehörenden Setup-Disketten und die Notfalldiskette sowie vorhandene Band-sicherungen durch sichere Aufbewahrung gegen unberechtigten Zugriff hinreichend geschützt?				M 4.77 M 4.49
120.05	Ist die Notfalldiskette auf einem aktuellen Stand?				M 4.77 M 642
120.06	Wird die Notfalldiskette nach jeder Konfigurati-onsänderung und nach jeder Installation eines Service Packs bzw. eines Hot Fixes aktualisiert?				M 4.76 M 6.42
120.07	Erfolgt die Aktualisierung der Notfalldiskette je-weils erst nach einem erfolgreichen Neustart des Systems?				M 4.76 M 6.42
120.08	Wird über die Aktualisierung der Notfalldiskette ein geeigneter Nachweis geführt?				M 4.76 M 6.42
120.09	Wird bei der Benutzung des Programms RDISK zunächst die Option „Notfall-Informationen aktua-lisieren“ gewählt, um den aktuellen Systemstand zu retten?				M 6.42
120.10	Sofern die Benutzerkonten und Zugriffsberechti-gungen mit auf der Notfalldiskette gesichert wer-den sollen: Wird die Notfalldiskette nach jeder Änderung an den Benutzerkonten und Zugriffsberechtigungen mit dem Programm RDISK unter Angabe des Pa-rameters /s gestartet?				M 6.42
120.11	Ist dem Administrationspersonal bekannt, wie im Notfall das System mit Hilfe der Reparaturdisket-				M 6.42

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	ten wiederhergestellt werden kann?				
120.12	**Für den Einsatz redundanter Windows NT Server**				
120.12.1	**Wie hoch sind die Verfügbarkeitsanforderungen für die Anwendungen auf dem untersuchten System?**				**M 6.43**
120.12.2	**Welche Abhängigkeit gibt es zwischen den auf dem System laufenden Anwendungen?**				**M 6.43**
120.12.3	**Welches ist die Anwendung mit den höchsten Verfügbarkeitsanforderungen?**				**M 6.43**
120.12.4	**In welcher Größenordnung können unter Berücksichtigung der Verfügbarkeitsanforderungen und der Abhängigkeiten Ausfälle toleriert werden?**				**M 6.43**
120.12.4.1	**Falls Ausfälle in der Größenordnung von 2 Tagen tolerierbar sind:**				**M 6.43**
120.12.4.1.1	**Wird ein RAID-Plattensystem eingesetzt?**				**M 6.43**
120.12.4.1.2	**Werden zusätzlich besonders wichtige Verzeichnisse auf einen anderen Rechner repliziert?**				**M 6.43**
	Ende {Falls Ausfälle in der Größenordnung von 2 Tagen tolerierbar sind:}				
120.12.4.2	**Falls Ausfälle in der Größenordnung von lediglich einer halben Stunde tolerierbar sind:**				**M 6.43**
120.12.4.2.1	**Steht ein separater Rechner zur Verfügung, der bei Ausfall des Servers dessen Aufgaben übernehmen kann?**				**M 6.43**
120.12.4.2.2	**Können bei Ausfall des Servers die Plattenlaufwerke auf den Ausweichrechner geschaltet werden?**				**M 6.43**
	Ende {Falls Ausfälle in der Größenordnung von lediglich einer halben Stunde tolerierbar sind:}				
120.12.4.3	**Falls Ausfälle in der Größenordnung von maximal einigen Minuten tolerierbar sind:**				
120.12.4.3.1	**Wird ein Cluster-System mit Zugriff aller Rechner auf alle Platten eingesetzt?**				**M 6.43**
120.12.4.3.2	**Ist das System so konfiguriert, dass bei Ausfall eines Servers automatisch auf einen Ersatzrechner**				**M 6.43**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	innerhalb des Systems umgeschaltet wird?				
	Ende {Falls Ausfälle in der Größenordnung von maximal einigen Minuten tolerierbar sind:}				
	Ende {Für den Einsatz redundanter Windows NT Server}				

130 Datensicherungskonzept

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
130.01	Besteht ein Datensicherungskonzept für das untersuchte System?				M 6.32
130.02	Welche Festlegungen enthält das Datensicherungskonzept hinsichtlich: Zeitintervall Zeitpunkt Anzahl der aufzubewahrenden Generationen Umfang der zu sichernden Daten Speichermedien Vorherige Löschung der Datenträger vor Wiederverwendung Zuständigkeit für die Durchführung Zuständigkeit für die Überwachung der Sicherung, insbesondere bei automatischer Durchführung Dokumentation der erstellten Sicherungen				M 6.32
130.03	Sind die Festlegungen hinsichtlich des Zeitintervalls und des Zeitpunkts der Datensicherungen sowie der Anzahl der aufzubewahrenden Generationen, des Umfangs der zu sichernden Daten sowie der zu verwendenden Speichermedien angemessen hinsichtlich der Menge und Wichtigkeit der laufend neu gespeicherten Daten und des möglichen Schadens der bei Verlust neuer Daten zwischen zwei Datensicherungen entsteht?				M 6.32 M 6.44
130.04	Werden die Datensicherungen konform zu den Festlegungen im Datensicherungskonzept durchgeführt?				M 6.32

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
130.05	**Wird der Datensicherungsvorgang dokumentiert?**				**M 6.44**
130.06	**Ist sichergestellt, dass alle Daten des untersuchten Systems gesichert werden?**				**M 6.32**
130.07	**Ist von der eingesetzten Software neben dem Originaldatenträger mindestens eine Sicherungskopie vorhanden?**				**M 6.32**
130.08	**Sind alle Produktionsdaten in die laufenden Datensicherungen einbezogen?**				**M 6.32**
130.09	**Wird unter Berücksichtigung des Datenvolumens und der Verfügbarkeitsanforderungen eine geeignete Software zur Datensicherung eingesetzt?**				**M 6.32** **M 6.44**
130.10	**Wird die Registrierung regelmäßig gesichert?**				**M 6.44**
130.11	**Werden die Sicherungsmedien, auf denen sich Datensicherungen befinden, sachgerecht gelagert?**				**M 6.44**
130.12	**Erfolgt die Lagerung der Sicherungsmedien, auf denen sich Datensicherungen befinden, außerhalb des Brandabschnittes, in dem sich das untersuchte System befindet (anzustreben ist stets die Aufbewahrung in einem anderen Gebäude)?**				**M 6.44**
130.13	**Ist sichergestellt, dass Unbefugte keinen Zugriff auf Sicherungsmedien haben?**				**M 6.44**
130.14	**Wird sachgemäß mit den Sicherungsmedien umgegangen?**				**M 6.44**
130.14.1	**Werden Viertelzoll-Bänder regelmäßig gespannt?**				**M 6.44**
130.14.2	**Wird beim Löschen von Datensicherungsbändern darauf geachtet, dass alle schutzwürdigen Daten eines Bandes physikalisch überschrieben werden?**				**M 6.44**
130.15	**Wird regelmäßig die Wiederherstellbarkeit der gesicherten Daten überprüft und sind diese Überprüfungen dokumentiert?**				**M 6.44**
130.16	**Ist bei vernetzten Systemen sichergestellt, dass auch die auf den Clients befindlichen Daten regelmäßig gesichert werden?**				**M 632**

140 Verschlüsselung

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
140.01	Welchen Schutzbedarf hinsichtlich des Wertes „Vertraulichkeit“ haben die Daten auf dem betrachteten System? (Ausschlaggebend sind die Daten mit dem höchsten Schutzbedarf).				M 5.36
140.02	Macht der Schutzbedarf eine Verschlüsselung der Daten bzw. von Nachrichten erforderlich?				M 5.36
140.02.1	Falls ja:				
140.02.1.1	Welche Verschlüsselungsverfahren und welche Produkte finden Anwendung				M 5.36
140.02.1.2	Wird – gemessen am Schutzbedarf und am Datenvolumen – ein geeignetes Verfahren / Produkt zur Verschlüsselung eingesetzt?				M 5.36
140.02.1.3	Werden die Benutzer im Umgang mit den eingesetzten Verschlüsselungsprodukten geschult?				M 5.36
140.02.1.4	Werden Daten und Schlüssel getrennt aufbewahrt?				M 5.36
	Ende {Macht der Schutzbedarf eine Verschlüsselung der Daten bzw. von Nachrichten erforderlich?}				

Befragte Person: Geprüft von: Datum:

150 Policy

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
150.01	Ist die für das Windows NT Netz erarbeitete Sicherheitsstrategie schriftlich dokumentiert und den Benutzern im notwendigen Umfang bekannt gemacht worden?				M 2.91
150.02	Wird die Sicherheitsstrategie an Veränderungen im Einsatzumfeld angepasst?				M 2.91
150.03	Gibt es für die Organisation einen übergeordneten Zeitplan für die auf allen Systemen durchzuführenden Sicherheitskontrollen u.a. mit Festlegung der Verantwortlichkeiten?				M 2.91
150.04	Wer ist zuständig für die Auswertung von Protokolldateien auf Servern bzw. Clients?				M 2.91
150.05	Wer ist auf Servern zuständig für die Vergabe von Freigabe- und NTFS-Berechtigungen?				M 2.91
150.06	Wer ist auf Workstations zuständig für die Vergabe von Freigabe- und NTFS-Berechtigungen?				M 2.91
150.07	Wer ist für die Überwachung der Hinterlegung und des Wechsels von PasswörtPasswörtern zuständig?				M 2.91
150.08	Wer ist für die Durchführung der Datensicherung auf den Servern verantwortlich?				M 2.91
150.09	Wer ist für die Durchführung der Datensicherung auf den Workstations verantwortlich?				M 2.91
150.10	Ist ein Verfahren festgelegt, wie auf sicherheitskritische Abweichungen reagiert werden soll?				M 2.92
150.11	Ist festgelegt, wer wann informiert werden soll?				M 2.92
150.12	Ist festgelegt, dass die abweichenden Einstellungen begründet wird und dass dargestellt werden muss, ob hierdurch eine Sicherheitslücke entsteht und welche Schritte ggf. zur Behebung der Sicherheitslücke erforderlich sind?				M 2.92
150.13	Wie wird auf Unregelmäßigkeiten reagiert?				M 2.92
150.14	Ist festgelegt, wer bei Unregelmäßigkeiten wann informiert wird?				M 2.92

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
150.15	**Werden Abweichungen der Sicherheitseinstellungen vom zulässigen Wert unverzüglich korrigiert?**				**M 2.92**
150.16	**Wird untersucht, ob eine Sicherheitslücke zu den Unregelmäßigkeiten geführt hat und wie die Sicherheitslücke behoben werden kann?**				**M 2.92**
150.17	**Wurde ein – gemessen am Schutzbedarf – sinnvolles Konzept für die Protokollierung erarbeitet?**				**M 2.91**

160 Benutzerorientierte Fragen

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
160.01	Ist ein Schulungskonzept für die Benutzer erarbeitet worden?				M 2.91
160.02	Wurden die Schulungen nach dem Konzept durchgeführt?				
160.03	Wird der Papierkorb regelmäßig gelöscht?				M 4.56
160.04	Sind die Benutzer des untersuchten Rechners darüber informiert, dass sensible Dateien nicht in den Papierkorb gezogen werden dürfen, sondern eine explizite Löschung durch Drücken der Umschalttaste beim Löschen erfolgen soll? Hinweis: Unter Benutzer in diesem Sinne sind alle Personen zu verstehen, die physikalisch Zugang zum untersuchten Rechner haben.				M 4.56
160.05	Sind alle Benutzer über die Regelungen zur Datensicherung informiert?				M 6.32
160.06	Ist bei vernetzten Systemen sichergestellt, dass auch die auf den Clients befindlichen Daten regelmäßig gesichert werden?				M 6.32
160.07	Sind die Benutzer darüber belehrt worden, bei gemeinsam benutzten Dateien möglichst an andere Benutzer nur die Zugriffsberechtigung „Ändern“ und nicht die Berechtigung „Vollzugriff“ zu vergeben?				M 4.53
160.08	Sind die Benutzer des untersuchten Systems darüber belehrt worden, regelmäßig mit dem Dateimanager oder dem Explorer zu überprüfen, ob sie noch Besitzer ihrer Verzeichnisse und Dateien sind?				M 4.53
160.09	Ist sichergestellt, dass die Eigentümer von Dateien und Verzeichnissen ihre Verpflichtung verstehen, anderen Benutzern auf diese Ressourcen nur dann Zugriff zu gewähren, wenn dies unbedingt erforderlich ist?				M 2.92
160.10	Falls das untersuchte System über ein Bandlauf-				

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	werk verfügt:				
160.10.1	**Befindet sich das untersuchte System in einer gesicherten Umgebung?**				**M 4.52**
160.10.1.1	**Falls nein:**				
160.10.1.1.1	**Wird der untersuchte Rechner jedes Mal neu gestartet, wenn das Bandlaufwerk benutzt wird?**				**M 4.52**
160.10.1.1.2	**Wird auf den Einsatz von selbstladenden Bandgeräten verzichtet?**				**M 4.52**
	Ende {Falls nein:}				
	Ende {Falls das untersuchte System über ein Bandlaufwerk verfügt:}				
160.11	**Bei der Benutzung von WfW oder Windows 95 im Windows NT Netz:**				
160.11.1	**Wird das Passwort-Caching eingesetzt?**				**M 5.40**
160.11.2	**Falls ja:**				
160.11.2.1	**Sind die Benutzer darüber belehrt worden, dass zusätzlich das Anmeldepasswort für den Schutz der individuellen Kennwortliste unter WfW bzw. Windows 95 notwendig ist?**				**M 5.40**
160.11.2.2	**Sind die Benutzer darüber belehrt worden, nur starke Passwörter zu benutzen?**				M 5.40
160.11.2.3	**Ist sichergestellt, dass bei der Anmeldung von Administratoren keine Passwortliste angelegt wird?**				**M 5.40**
	Ende {Falls ja:}				
	Ende {Bei der Benutzung von WfW oder Windows 95 im Windows NT Netz:}				

200 Domänenkonzept

210 Netzstruktur

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
210.01	Ist die gewählte Windows NT-Netzstruktur dokumentiert?				M 2.93
210.02	Sind die Gründe, die zu der Wahl der Netzstruktur geführt haben, dokumentiert?				M 2.93
210.03	Wird die Netzstruktur an Änderungen im Einsatzumfeld angepasst?				M 2.93
210.04	Ist der Grundsatz beachtet worden, nicht mehr Server als notwendig zu installieren?				M 2.93
210.05	Wird auf die Nutzung dedizierter Windows NT Server verzichtet?				M 2.93
210.05.1	Falls nein:				
210.05.1.1	Wie viele dedizierte Server gibt es innerhalb der untersuchten Organisation?				M 2.93
210.05.1.2	Welche zwingenden Gründe gibt es, die dagegen sprechen, diese Server in eine Domäne einzubinden?				M 2.93
	Ende {Verzicht auf die Benutzung dedizierter Windows NT Server}				
210.06	Sofern auf das betrachtete System Zugriffe von DOS-PCs (einschließlich Windows 3.x und Windows 95) erfolgen:				
210.06.1	Ist der Einsatz von PCs, die mit dem Betriebssystem MS-DOS (einschließlich Windows 3.x und Windows 95) arbeiten, unabdingbar?				M 5.40
210.06.1.1	Falls ja:				
210.06.1.1.1	Ist sichergestellt, dass nur die berechtigten Benutzer Zugang zu PCs mit dem Betriebssystem MS-DOS haben?				M 5.40
210.06.1.1.2	Werden alle Türen von Büros, in denen DOS-PCs untergebracht sind, bei Abwesenheit der entsprechenden Mitarbeiter verschlossen?				M 5.40
210.06.1.1.3	Sind zu diesen Räumen Zutrittsberechtigungen vergeben worden und wird die Einhaltung dieser Berechtigungen regelmäßig kontrolliert?				M 5.40

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
210.06.1.1.4	**Ist sichergestellt, dass auf diesen Rechnern Software nicht unkontrolliert eingespielt werden kann?**				**M 5.40**
210.06.1.1.5	**Gibt es ein explizites, schriftliches Nutzungsverbot nicht freigegebener Software für diese Rechner?**				**M 5.40**
210.06.1.1.6	**Wird der Softwarebestand auf diesen Rechnern regelmäßig geprüft?**				**M 5.40**
210.06.1.1.7	**Wird auf diesen Rechnern regelmäßig ein Virenschutzprogramm eingesetzt?**				**M 5.40**
210.06.1.1.8	**Sind die Rechner über das BIOS so konfiguriert, dass das Booten über das Diskettenlaufwerk oder das CD-ROM-Laufwerk nicht möglich ist?**				**M 5.40**
210.06.1.1.9	**Ist diese Einstellung per BIOS-Passwort abgesichert?**				**M 5.40**
	Ende {Ist der Einsatz von PCs, die mit dem Betriebssystem MS-DOS (einschließlich Windows 3.x und Windows 95) arbeiten, unabdingbar?}				
	Ende {Sofern auf das betrachtete System Zugriffe von DOS-PCs (einschließlich Windows 3.x und Windows 95) erfolgen:}				

220 Domänenstruktur und Verwaltung

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
220.01	**Falls Domänen eingerichtet wurden:**				
220.01.1	**Wie viele Domänen wurden eingerichtet?**				**M 2.93**
220.01.2	**Wurde der Grundsatz beachtet, möglichst wenig Domänen zu bilden?**				**M 2.93**
220.01.3	**Ist die Anzahl der primären Domänencontroller im Hinblick auf die Anzahl der in der Domäne zu verwaltenden Benutzer- und Computerkonten angepasst?**				**M 2.93**
220.01.4	**Wurden Server als Backup Domänencontroller installiert?**				**M 2.93**
220.01.5	**Ist die Anzahl der Backup Domänencontroller im Hinblick auf die Anzahl der in der Domäne zu verwaltenden Benutzer- und Computerkonten angepasst?**				**M 2.93**
220.01.6	**Wurden alle Rechner als Mitglied einer Domäne konfiguriert?**				**M 4.55**
220.01.7	**Wurde darauf verzichtet, Rechner als Mitglied von Arbeitsgruppen zu konfigurieren?**				**M 2.93a** **M 4.55**
220.01.7.1	**Falls nein:**				
220.01.7.1.1	**Gibt es zwingende Gründe, die die Einrichtung von Arbeitsgruppen neben den bestehenden Domänen rechtfertigen?**				**M 2.93** **M 4.55**
220.01.7.1.2	**Sind die Nachteile durch Nutzung der Peer-to-Peer-Funktionen (z.B. unübersichtliche Rechtestrukturen) hinnehmbar?**				**M 2.93**
220.01.7.1.3	**Kann auf eine zentrale Administration verzichtet werden?**				**M 2.93**
	Ende {Wurde darauf verzichtet, Rechner als Mitglied von Arbeitsgruppen zu konfigurieren?}				
220.01.8	**Wird bei Rechnern, die einer Domäne angehören, darauf verzichtet, lokale Benutzerkonten anzulegen?**				**M 4.55**

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
220.01.9	**Sind Peer-to-Peer-Funktionen in der betrachteten Organisation zugelassen, d.h. sind Freigaben auf den einzelnen Workstations möglich?**				**M 2.91** **M 5.37**
220.01.9.1	**Falls ja:**				
220.01.9.1.1	**Entspricht die Zulassung von Peer-to-Peer-Funktionen den Festlegungen in der Sicherheitspolitik?**				**M 2.91** **M 5.37**
220.01.9.1.2	**Sind die zugelassenen Peer-to-Peer-Funktionen auf das absolute Minimum beschränkt?**				**M 2.91** **M 5.37**
	Ende {Sind Peer-to-Peer-Funktionen in der betrachteten Organisation zugelassen, d.h. sind Freigaben auf den einzelnen Workstations möglich?}				
220.01.10	**Falls auf dem primären bzw. dem/den Backup Domänencontroller(n) extrem zeitkritische Aufgaben oder umfangreiche Applikationen ausgeführt werden:**				
220.01.10.1	**Sind Störungen durch mangelnde Performance aufgrund dieser Konstellation ausgeschlossen? Hinweis: Ggf. ist eine Installation der Aufgaben/Applikationen auf Memberservern vorzusehen!**				**M 2.93**
	Ende {Falls auf dem primären bzw. dem/den Backup Domänencontroller(n) extrem zeitkritische Aufgaben oder umfangreiche Applikationen ausgeführt werden:}				
	Ende {Falls Domänen eingerichtet wurden:}				

230 Vertrauensbeziehungen

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
230.01	**Falls es Vertrauensbeziehungen zwischen Domänen gibt:**				
230.01.1	**Ist jede dieser Vertrauensbeziehungen zwingend notwendig?**				**M 2.94**
230.01.2	**Sind die Vertrauensbeziehungen zwischen Domänen dokumentiert?**				**M 2.93**
230.01.3	**Werden Vertrauensbeziehungen zwischen Domänen an Änderungen im Einsatzumfeld angepasst?**				**M 2.93**
	Ende {Falls es Vertrauensbeziehungen zwischen Domänen gibt:}				

Befragte Person: Geprüft von: Datum:

300 Installation und Konfiguration

310 Sicheres Betriebssystem

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
310.01	Welche Sprachversion von Windows NT wurde bei dem untersuchten System installiert?				M 4.76 M 4.55
310.02	Sind die Gründe für die Auswahlentscheidung Sprachversion nachvollziehbar dokumentiert?				M 4.76 M 4.55
310.03	Sind die angeführten Gründe stichhaltig und nachvollziehbar?				M 4.76 M 4.55
310.04	Ist Windows NT mindestens in der Version 3.51 auf dem System installiert?				M 4.76 M 4.55
310.05	Wird die Systemintegrität regelmäßig überprüft?				M 2.92
310.05.1	Wie erfolgt diese Prüfung?				M 2.92
310.05.2	Werden die Daten der letzten Veränderung wichtiger Systemdateien in die Überprüfung mit einbezogen?				M 2.92
310.05.3	Wird die Veränderung der Zugriffsrechte wichtiger Systemdateien in die Überprüfung mit einbezogen?				M 2.92
310.05.4	Wer ist für diese Prüfungen zuständig?				M 2.92
310.05.5	Wie lang ist ein Prüfungsintervall?				M 2.92
310.05.6	Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?				M 2.92
310.05.7	Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?				M 2.92
310.05.8	Werden diese Prüfungen dokumentiert?				M 2.92
310.06	Ist sichergestellt, dass Service Packs bzw. Hot Fixes vor der Installation auf dem Produktionssystem auf einem entsprechend konfigurierten Test-System getestet werden?				M 4.76
310.07	Wie ist sichergestellt, dass nach jeder Änderung der Systemkonfiguration, die einen Zugriff auf die Installations-CD-ROM erforderlich macht, bzw. nach der Installation von neuen Gerätetreibern das aktuelle Service Pack und die notwendigen Hot				M 4.76

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	Fixes erneut installiert werden? Hinweis: Denkbar ist u.a. eine schriftliche Anweisung an den Administrator.				
310.08	**Wird ein geeigneter Nachweis über die erneute Installation des aktuellen Service Packs und der notwendigen Hot Fixes geführt?**				**M 4.76**
310.09	**Ist sichergestellt, dass nach der Installation eines Service Packs bzw. eines Hot Fixes die Sicherheitskonfiguration des betrachteten Systems überprüft wird?**				**M 4.76**
310.09.1	**Werden diese Überprüfungen in geeigneter Weise dokumentiert?**				**M 4.76**
310.10	**Falls Windows NT in der Version 3.51 installiert wurde:**				
310.10.1	**Ist das Service Pack 5 installiert? Hinweis: Sofern das aktuelle Service Pack nicht installiert wurde, müssen die Gründe nachvollziehbar durch den Verantwortlichen dargelegt werden.**				**M 4.76 M 4.55**
	Ende {Falls Windows NT in der Version 3.51 installiert wurde:}				
310.11	**Falls Windows NT in der Version 4.0 installiert wurde:**				
310.11.1	**Ist das aktuelle Service Pack installiert (zum Stichtag 04.08.1999 für Windows NT 4.0 das Service Pack 5)? Hinweis: Sofern das aktuelle Service Pack nicht installiert wurde, müssen die Gründe nachvollziehbar durch den Verantwortlichen dargelegt werden.**				**M 4.76 M 4.55**
310.11.2	**Welche Hot Fixes sind auf dem betrachteten System installiert worden?**				**M 4.76**
310.11.3	**Entspricht die Installation der Hot Fixes den Festlegungen in der Sicherheitspolicy?**				
310.11.4	**Sind – orientiert an den benutzten Diensten und Protokollen sowie der eingesetzten Hardware – die**				**M 4.76**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	für das System notwendigen Hot Fixes installiert?				
310.11.5	**Wurde darauf verzichtet, zusätzliche, d.h. für die Funktionalität des Systems nicht zwingend benötigte Hot Fixes zu installieren?**				**M 4.76**
310.11.6	**Falls bei dem betrachteten System unter Windows NT 4.0 auf die Installation des Service Packs 4 und höher verzichtet wurde:**				
310.11.6.1	**Ist der Hot Fix „getadmin-fix“ auf dem betrachteten System installiert worden, sofern die Windows NT Version 4.0 zum Einsatz kommt?**				**M 4.77**
	Ende {Falls bei dem betrachteten System unter Windows NT 4.0 auf die Installation des Service Packs 4 und höher verzichtet wurde:}				
310.11.7	**Falls Server fernadministriert werden:**				
310.11.7.1	**Ist auf den Rechnern, über die die Fernadministration erfolgt, mindestens das Service Pack 3 und der Hot Fix „lm-fix“ bzw. das aktuelle Service Pack (z.Zt. Service Pack 5) installiert?**				**M 4.77**
	Ende {Falls Server fernadministriert werden:}				
	Ende {Falls Windows NT in der Version 4.0 installiert wurde:}				

320 Installierte Komponenten

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
320.01	Werden alle Partitionen unter dem Filesystem NTFS betrieben?				M 4.55 M 4.53
320.01.1	Falls Nein				
320.01.1.1	Aus welchen Gründen wird auf das Filesystem NTFS verzichtet?				M 4.55
320.01.1.2	Sind diese Gründe nachvollziehbar und ist der Betrieb unter einem anderen Filesystem als NTFS unter Sicherheitsgesichtspunkten vertretbar?				M 4.55
	Ende {Werden alle Partitionen unter dem Filesystem NTFS betrieben?}				
320.02	Ist sichergestellt, dass auf den Festplatten des betrachteten Systems keine anderen Betriebssysteme außer Windows NT installiert sind?				M 4.49 M 4.56
320.02.1	Wird diese Vorgabe regelmäßig überprüft?				M 4.49
320.02.2	Wer ist für diese Prüfungen zuständig?				M 4.49
320.02.3	Wie lang ist ein Prüfungsintervall?				M 4.49
320.02.4	Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?				M 4.49
320.02.5	Werden diese Prüfungen dokumentiert?				M 4.49
320.03	Falls das Subsystem POSIX installiert ist:				
320.03.1	Ist die Installation dieses Subsystems im Sicherheitskonzept vorgesehen?				M 4.55
320.03.2	Wird das Subsystem POSIX zwingend benötigt?				M 4.55
320.03.3	Sind – gemessen am Schutzbedarf – die Risiken, die der Einsatz bedeutet, hinnehmbar?				M 4.55
	Ende {Falls das Subsystem POSIX installiert ist:}				
320.04	Falls das Subsystem POSIX nicht benötigt wird:				M 4.55

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
320.04.1	**Wurde auf die Installation des Subsystems POSIX verzichtet?**				**M 4.55**
320.04.2	**Wurde das Unterverzeichnis POSIX im Verzeichnis *%Systemroot%*\SYSTEM32 gelöscht?**				**M 4.55**
320.04.3	**Wurden folgende Bibliotheken im Verzeichnis *%Systemroot%*\SYSTEM32 gelöscht? - PSXDLL.DLL - PAX.EXE - POSIX.EXE - PSXSS.EXE**				**M 4.55**
	Ende {Falls das Subsystem POSIX <u>nicht</u> benötigt wird:}				
320.05	**Falls das Subsystem OS/2 installiert ist:**				
320.05.1	**Ist die Installation dieses Subsystems im Sicherheitskonzept vorgesehen?**				**M 4.55**
320.05.2	**Wird das Subsystem OS/2 zwingend benötigt?**				
320.05.3	**Sind – gemessen am Schutzbedarf – die Risiken, die der Einsatz bedeutet, hinnehmbar?**				**M 4.55**
	Ende {Falls das Subsystem OS/2 installiert ist:}				
320.06	**Falls das Subsystem OS/2 <u>nicht</u> benötigt wird:**				**M 4.55**
320.06.1	**Wurde auf die Installation des Subsystems OS/2 verzichtet?**				**M 4.55**
320.06.2	**Wurde das Unterverzeichnis OS2 im Verzeichnis *%Systemroot%*\SYSTEM32 gelöscht?**				**M 4.55**
320.06.3	**Wurden folgende Bibliotheken im Verzeichnis *%Systemroot%*\SYSTEM32 gelöscht? OS2.EXE OS2SRV.EXE OS2SS.EXE**				**M 4.55**
	Ende {Falls das Subsystem OS/2 <u>nicht</u> benötigt wird:}				

330 Konfiguration

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
330.01	**Ist der maximal reservierte Speicherbereich für den Papierkorb auf einen möglichst kleinen Wert festgelegt (z.B. 2 MB)?**				**M 4.56**

Befragte Person: Geprüft von: Datum:

340 Hardwareinstallation

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
340.01	**Nur Systeme, die über mindestens ein Disketten-laufwerk verfügen:**				
340.01.1	**Falls es sich um einen Server handelt:**				**M 4.49**
340.01.1.1	**Ist das Diskettenlaufwerk durch ein Disketten-schloss gesperrt?**				**M 4.49**
	Ende {Falls es sich um einen Server handelt:}				
340.01.2	**Bei sonstigen Systemen:**				
340.01.2.1	**Steht der Rechner in einer gesicherten Umgebung unter strikter physischer Kontrolle, d. h. ist sicher-gestellt, dass kein Unbefugter Zugriff auf den Rechner nehmen kann?**				**M 4.49**
340.01.2.1.1	**Falls nein:**				
340.01.2.1.2	**Ist das Diskettenlaufwerk durch ein Disketten-schloss gesperrt?**				**M 4.49**
340.01.2.1.3	**Falls das Diskettenlaufwerk nicht für die tägliche Arbeit benötigt wird:**				
340.01.2.1.3.1	**Sind Diskettenlaufwerke über die Systemsteue-rungsoption „*Geräte*“ Gerät „*Floppy*“ deaktiviert?**				**M 4.49**
	Ende {Wird das Diskettenlaufwerk für die tägliche Arbeit zwingend benötigt?}				
	Ende {Steht der Rechner in einer gesicherten Um-gebung unter strikter physischer Kontrolle, d. h. ist sichergestellt, dass kein Unbefugter Zugriff auf den Rechner nehmen kann?}				
	Ende {Sonstige Systeme}				
340.01.3	**Alle Systeme:**				
340.01.3.1	**Wie häufig wird die Sicherung der Diskettenlaufwerke ge-prüft?**				**M 4.49**
340.01.3.2	**Wer ist für diese Prüfung zuständig?**				**M 4.49**

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
340.01.3.3	**Wie lang ist ein Prüfungsintervall?**				**M 4.49**
340.01.3.4	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 4.49**
340.01.3.5	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 4.49**
340.01.3.6	**Werden diese Prüfungen dokumentiert?**				**M 4.49**
340.01.3.7	**Ist durch eine entsprechende Einstellung im BIOS sichergestellt, dass auf dem betrachteten System weder von CD-ROM-Laufwerken noch von Disketten-laufwerken ein anderes Betriebssystem gebootet werden kann?**				**M 4.49**
340.01.3.7.1	**Wurde das BIOS durch ein entsprechendes Passwort geschützt?**				**M 4.49**
340.01.3.7.2	**Werden diese BIOS-Einstellungen regelmäßig geprüft?**				**M 4.49**
340.01.3.7.3	**Wer ist für diese Prüfungen zuständig?**				**M 4.49**
340.01.3.7.4	**Wie lang ist ein Prüfungsintervall?**				**M 4.49**
340.01.3.7.5	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 4.49**
340.01.3.7.6	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 4.49**
340.01.3.7.7	**Wurden diese Prüfungen dokumentiert?**				**M 4.49**
	Ende {Nur Systeme, die über mindestens ein Diskettenlaufwerk verfügen:}				
340.02	**Falls das betrachtete System mit einem Rechnermikrofon ausgestattet ist:**				
340.02.1	**Wird das Rechnermikrofon zwingend aus dienstlichen/betrieblichen Gründen benötigt?**				**M 4.40**
340.02.1.1	**Falls ja:**				
340.02.1.1.1	**Ist festgelegt, wer das Rechnermikrofon aktivieren darf?**				**M 4.40**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
340.02.1.2	**Sonst falls nein:**				
340.02.1.2.1	**Ist durch Ausschalten oder physikalische Trennung des Mikrofons vom Rechner oder – soweit dies nicht möglich – zumindest durch Entziehen der Zugriffsrechte auf die entsprechenden Schlüssel der Registrierung im Bereich HKEY_LOCAL_MACHINE\HARDWARE\ sichergestellt, dass das Rechnermikrofon nicht unberechtigt genutzt werden kann?**				**M 4.40**
	Ende {Wird das Rechnermikrofon zwingend aus dienstlichen/betrieblichen Gründen benötigt?}				
	Ende {Falls das betrachtete System mit einem Rechnermikrofon ausgestattet ist:}				

400 Protokolle und Dienste

410 Installierte Protokolle

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
410.01	**Welche Protokolle sind auf dem betrachteten System installiert worden?**				
410.02	**Wurde der Grundsatz beachtet, nur die zwingend benötigten Protokolle zu installieren?**				

Befragte Person: Geprüft von: Datum:

420 Installierte Dienste

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
410.01	Welche Dienste sind auf dem betrachteten System installiert?				M 4.55
410.02	Sind nur solche Dienste installiert, die auch im Sicherheitskonzept / Konfigurationskonzept vorgesehen sind?				M 4.55
410.03	Wird auf die Ausführung von Diensten, die keine Standarddienste von Windows NT sind, verzichtet?				M 4.55
410.03.1	Falls nein:				
410.03.1.1	Um welche Dienste handelt es sich?				M 4.55
410.03.1.2	Ist die Ausführung dieser Dienste zwingend notwendig?				M 4.55
410.03.1.3	Ist sichergestellt, dass diese Dienste unter einem Benutzerkonto und nicht im Kontext Betriebssystem gestartet werden?				M 4.55
410.03.1.3.1	Falls ja:				
410.03.1.3.1.1	Ist sichergestellt, dass diese Benutzerkonten zu keinem anderen Zweck benutzt werden?				M 4.55
410.03.1.3.1.2	Ist sichergestellt, dass kein Benutzer diese Konten zur Anmeldung benutzt?				M 4.55
410.03.1.3.2	Sonst falls nein:				
410.03.1.3.2.1	Welche zwingenden Gründe gibt es, diese Dienste im Kontext Betriebssystem zu starten?				M 4.55
	Ende {Ist sichergestellt, dass diese Dienste unter einem Benutzerkonto und nicht im Kontext Betriebssystem gestartet werden?}				
	Ende {Wird auf die Ausführung von Diensten, die keine Standarddienste von Windows NT sind, verzichtet?}				
410.04	Falls der RAS-Dienst eingesetzt wird:				
410.04.1	Wird für die Authentisierung zwischen dem RAS-Server und dem RAS-Client das Authentisierungs-				M 5.41

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	protokoll CHAP und MD5 eingesetzt?				
410.04.2	**Ist für die Benutzer mit RAS-Berechtigung die Callback-Option eingeschaltet?**				**M 5.41**
410.04.3	**Ist für jeden Benutzer die Rufnummer am Server eingetragen, an die der Rückruf des Servers gehen soll?**				**M 5.41**
410.04.4	**Ist der RAS-Zugriff für die Benutzer so konfiguriert, dass lediglich Ressourcen auf dem RAS-Server für den Remote-Zugriff zur Verfügung stehen, d.h. ist ein Durchgriff auf das restliche Netz ausgeschlossen?**				**M 5.41**
410.04.5.1	**Werden diese Einstellungen regelmäßig überprüft?**				**M 5.41**
410.04.5.2	**Wer ist für diese Prüfungen zuständig?**				**M 5.41**
410.04.5.3	**Wie lang ist ein Prüfungsintervall?**				**M 5.41**
410.04.5.4	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 5.41**
410.04.5.5	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 5.41**
410.04.5.6	**Werden diese Prüfungen dokumentiert?**				**M 5.41**
410.04.6	**Ist sichergestellt, dass nach Änderung der RAS-Berechtigungen sofort eine Synchronisation der Domäne durchgeführt wird?**				**M 5.41**
	Ende {Wird der RAS-Dienst eingesetzt?}				
410.05.1	**Ist im Sicherheitskonzept der Organisation festgelegt, welche Netzdienste zum Einsatz kommen sollen?**				**M 5.42**
410.05.2	**Ist für jeden Netzdienst eine detaillierte Sicherheitsanalyse durchgeführt worden?**				**M 5.42**
410.05.3	**Sind nur die minimal erforderlichen Netzdienste zur Installation und zum Betrieb vorgesehen worden?**				**M 5.42**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
410.05.4	**Wird jeder Netzdienst regelmäßig daraufhin überprüft, ob die Benutzung noch zwingend notwendig ist?**				**M 5.42**
410.05.4.1	**Wer ist für diese Prüfung verantwortlich?**				**M 5.42**
410.05.4.2	**Wie lang ist ein Prüfungsintervall?**				**M 5.42**
410.05.4.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 5.42**
410.05.4.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 5.42**
410.05.4.5	**Werden diese Prüfungen dokumentiert?**				**M 5.42**
410.05.5	**Welche Netzdienste sind auf dem betrachteten System installiert?**				**M 5.42**
4.10.05.5.1	**Sind nur die Dienste installiert, die im Sicherheitskonzept vorgesehen sind?**				**M 5.42**
410.05.5.2	**Sind die einzelnen Parameter für die Installation und den Betrieb der Netzdienste schriftlich festgelegt?**				**M 5.42**
410.05.5.3	**Falls auf dem betrachteten System der DHCP-Dienst installiert ist:**				
410.05.5.3.1	**Sind die Administratoren darüber belehrt, die Dateien DHCP.TMP, DHCP.MDB, JET.LOG und SYSTEM.MDB nicht zu ändern oder zu löschen?**				**M 5.42**
410.05.5.3.2	**Entspricht die Konfiguration des DHCP-Dienstes den Vorgaben des Sicherheitskonzeptes bzw. den Maßnahmenempfehlungen aus der Sicherheitsanalyse?**				**M 5.42**
	Ende {Falls auf dem betrachteten System der DHCP-Dienst installiert ist:}				
410.05.5.4	**Falls auf dem betrachteten System der WINS-Dienst installiert ist:**				
410.05.5.4.1	**Wieviele WINS-Server sind im Netz der betrachteten Organisation eingerichtet?**				**M 5.42**
410.05.5.4.2	**Ist der Parameter für die Reproduktion unter Berücksichtigung der entstehenden Netzlast, der**				**M 5.42**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	geographischen Verhältnisse und der Häufigkeit von Änderungen angemessen gewählt?				
410.05.5.4.3	**Sind die Administratoren darüber belehrt, die Dateien JET.LOG, SYSTEM.MDB, WINS.MDB und WINSTMP.MDB weder zu löschen noch zu verändern?**				**M 5.42**
410.05.5.4.4	**Entspricht die Konfiguration des WINS-Dienstes den Vorgaben des Sicherheitskonzeptes bzw. den Maßnahmenempfehlungen aus der Sicherheitsanalyse?**				**M 5.42**
410.05.5.4.5	**Wird die Konfiguration des WINS-Dienstes regelmäßig überprüft?**				**M 5.42**
410.05.5.4.5.1	**Wer ist für diese Prüfungen zuständig?**				**M 5.42**
410.05.5.4.5.2	**Wie lang ist ein Prüfungsintervall?**				**M 5.42**
410.05.5.4.5.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 5.43**
410.05.5.4.5.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 5.42**
410.05.5.4.5.5	**Wurden diese Prüfungen dokumentiert?**				**M 5.42**
	Ende {Falls auf dem betrachteten System der WINS-Dienst installiert ist:}				
410.05.5.5	**Falls auf dem betrachteten System der SNMP-Dienst installiert ist:**				
410.05.5.5.1	**Ist die Konfiguration von SNMP schriftlich im Sicherheitskonzept festgelegt?**				**M 5.42**
410.05.5.5.2	**Entspricht die Installation von SNMP auf dem betrachteten Rechner diesen Festlegungen?**				**M 5.42**
410.05.5.5.3	**Sind die Communities und Hosts festgelegt, von denen ein Computer Anforderungen entgegennimmt?**				**M 5.42**
410.05.5.5.4	**Wird ein Echtheitsbestätigungs-Trap gesendet, wenn eine Community oder ein Host unberechtigterweise Informationen anfordert?**				**M 5.42**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
410.05.5.5.5	**Ist SNMP so konfiguriert, dass es nur Anforderungen definierter Communities annimmt, d. h. ist ausgeschlossen, dass Anforderungen der vordefinierten Community *public* angenommen werden?**				**M 5.42**
410.05.5.5.6	**Werden die entsprechenden Protokolle regelmäßig ausgewertet?**				**M 5.42**
410.05.5.5.6.1	**Wie lang ist ein Überprüfungsintervall?**				**M 5.42**
410.05.5.5.6.2	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 5.42**
410.05.5.5.6.3	**Entspricht die Intervallänge dem Schutzbedarf des untersuchten Systems?**				**M 5.42**
410.05.5.5.6.4	**Wer ist für die Überprüfung verantwortlich?**				**M 5.42**
	Ende {Falls auf dem betrachteten System der SNMP-Dienst installiert ist:}				
410.06.1	**Ist im Sicherheitskonzept der Organisation festgelegt, welche TCP/IP-Netzdienste zum Einsatz kommen sollen?**				**M 5.43**
410.06.2	**Ist für jeden Netzdienst eine detaillierte Sicherheitsanalyse durchgeführt worden?**				
410.06.3	**Sind nur die minimal erforderlichen TCP/IP-Netzdienste zur Installation und zum Betrieb vorgesehen worden?**				**M 5.43**
410.06.4	**Wird jeder TCP/IP-Netzdienst regelmäßig daraufhin überprüft, ob die Benutzung noch zwingend notwendig ist?**				**M 5.43**
410.06.4.1	**Wer ist für diese Prüfung verantwortlich?**				**M 5.43**
410.06.4.2	**Wie lang ist ein Prüfungsintervall?**				**M 5.43**
410.06.4.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 5.43**
410.06.4.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 5.43**
410.06.4.5	**Werden die Ergebnisse dieser Prüfungen dokumentiert?**				**M 5.43**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
410.06.5	**Welche TCP/IP-Netzdienste sind auf dem betrachteten System installiert?**				**M 5.42**
410.06.6	**Sind nur die Dienste installiert, die im Sicherheits-konzept vorgesehen sind?**				**M 5.43**
410.06.7	**Sind die einzelnen Parameter für die Installation und den Betrieb der TCP/IP-Netzdienste schriftlich festgelegt worden?**				**M 5.43**
410.06.8	**Verfügt der betrachtete Rechner über eine Verbindung zu einem externen Netz und verfügt er über mehrere Netzwerkkarten oder ist der Fernzugriff über RAS installiert?**				**M 5.43**
410.06.8.1	**Falls ja:**				
410.06.8.1.1	**Ist darauf verzichtet worden, die Option „*IP-Forwarding aktivieren*“ auf der Registerkarte „*Routing*“ einzuschalten?**				**M 5.43**
410.06.8.1.2	**Ist für die einzelnen Netzwerkkarten die Option „Sicherheit aktivieren“ eingeschaltet?**				**M 5.43**
410.06.8.1.3	**Ist im Rahmen einer Sicherheitsanalyse festgelegt worden, welche TCP- und UDP-Anschlüsse freigegeben bzw. gesperrt werden?**				**M 5.43**
410.06.8.1.4	**Entspricht die Konfiguration der Anschlüsse auf dem betrachteten Rechner diesen Vorgaben?**				**M 5.43**
	Ende {Verfügt der betrachtete Rechner über eine Verbindung zu einem externen Netz und verfügt er über mehrere Netzwerkkarten oder ist der Fernzugriff über RAS installiert?}				
410.06.9	**Falls auf dem untersuchten System der FTP-Dienst zum Einsatz kommt:**				**M 5.43**
410.06.9.1	**Ist der Einsatz des FTP-Dienstes zur Übertragung von Daten zwingend erforderlich? Hinweis: In reinen Windows NT Netzen wird der FTP-Dienst nicht benötigt und sollte daher deinstalliert werden!**				**M 5.43**
410.06.9.2	**Entspricht die Konfiguration des FTP-Dienstes den Festlegungen im Sicherheitskonzept bzw. den Maßnahmenempfehlungen der Sicherheits-**				**M 5.43**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	analyse?				
410.06.9.3	**Wird die Notwendigkeit und die Konfiguration dieses Dienstes regelmäßig überprüft?**				**M 5.43**
410.06.9.3.1	**Wie häufig finden diese Überprüfungen statt?**				**M 5.43**
410.06.9.3.2	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 5.43**
410.06.9.3.3	**Entspricht die Länge des Überprüfungsintervalls dem festgestellten Schutzbedarf?**				**M 5.43**
410.06.9.3.4	**Wer ist für diese Überprüfungen zuständig?**				**M 5.43**
410.06.9.4	**Wird ausschließlich anonymes FTP zugelassen?**				**M 5.43**
410.06.9.5	**Werden eingehende FTP-Verbindungen protokolliert?**				**M 5.43**
410.06.9.6	**Werden die entsprechenden Protokolle regelmäßig ausgewertet?**				**M 5.43**
410.06.9.6.1	**Wer ist für die Überprüfung verantwortlich?**				**M 5.43**
410.06.9.6.2	**Wie lang ist ein Überprüfungsintervall?**				**M 5.43**
410.06.9.6.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 5.43**
410.06.9.6.4	**Entspricht die Intervalllänge dem Schutzbedarf des untersuchten Systems?**				**M 5.43**
410.06.9.6.5	**Werden diese Prüfungen dokumentiert?**				**M 5.43**
410.06.9.7	**Falls FTP im WAN eingesetzt wird:**				**M 5.43**
410.06.9.7.1	**Ist das lokale Netz durch eine Firewall geschützt?**				**M 5.43**
410.06.9.7.2	**Sind anonyme Verbindungen nur auf speziell hierfür eingerichteten Systemen erlaubt?**				**M 5.43**
410.06.9.7.3	**Ist sichergestellt, dass auf diesen Systemen keine anderen Informationen als nur die, die über FTP angeboten werden, gespeichert sind?**				**M 5.43**
	Ende {Falls FTP im WAN eingesetzt wird:}				

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	Ende {Falls auf dem untersuchten System der FTP-Dienst zum Einsatz kommt:}				
410.06.10	**Falls auf dem untersuchten System ein Telnet-Server installiert wurde:**				**M 5.43**
410.06.10.1	**Ist das Netz zuverlässig gegen Abhören geschützt?**				**M 5.43**
410.06.10.2	**Ist der Telnet-Server-Dienst zwingend erforderlich? Hinweis: Sofern der Telnet-Server-Dienst nicht benötigt wird, sollte dieser deinstalliert werden!**				**M 5.43**
410.06.10.3	**Wird die Notwendigkeit dieses Dienstes regelmäßig überprüft?**				**M 5.42**
410.06.10.3.1	**Wie häufig finden diese Überprüfungen statt?**				**M 5.42**
410.06.10.4.2	**Entspricht die Länge des Überprüfungsintervalls dem festgestellten Schutzbedarf?**				**M 5.42**
410.06.10.3.3	**Wer ist für diese Überprüfungen zuständig?**				**M 5.43**
410.06.10.4	**Entspricht die Konfiguration des Telnet-Server-Dienstes den Festlegungen in der Sicherheitsstrategie?**				**M 5.43**
410.06.10.5	**Wird die Konfiguration des Telnet-Server-Dienstes regelmäßig überprüft?**				**M 5.43**
410.06.10.5.1	**Wer ist für diese Prüfungen zuständig?**				**M 5.43**
410.06.10.5.2	**Wie lang ist ein Prüfungsintervall?**				**M 5.43**
410.06.10.5.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 5.43**
410.06.10.5.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 5.43**
410.06.10.5.5	**Werden diese Prüfungen dokumentiert?**				**M 5.43**
	Ende {Falls auf dem untersuchten System ein Telnet-Server installiert wurde:}				
410.06.11	**Falls auf dem untersuchten System der NFS-Dienst installiert ist:**				
410.06.11.1	**Ist auf dem betrachteten Server der NFS-Dienst zwingend erforderlich?**				**M 5.42**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	Hinweis: Wenn der NFS-Dienst nicht zwingend benötigt wird, sollte dieser deinstalliert werden!				
410.06.11.2	**Wird die Notwendigkeit dieses Dienstes regelmäßig überprüft?**				**M 5.42**
410.06.11.2.1	**Wie häufig finden diese Überprüfungen statt?**				**M 5.42**
410.06.11.2.2	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 5.42**
410.06.11.2.3	**Entspricht die Länge des Überprüfungsintervalls dem festgestellten Schutzbedarf?**				**M 5.42**
410.06.11.2.4	**Wer ist für diese Überprüfungen zuständig?**				**M 5.43**

500 Benutzermanagement

510 Benutzer- und Gruppenverwaltung

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
510.01	Gibt es ein schlüssiges Konzept für die Bildung von Benutzerkonten?				M 2.19
510.02	Ist danach die Zuordnung von Benutzern auf vordefinierte und frei definierte Benutzergruppen schriftlich festgelegt?				M 4.50
510.03	Welche Namenkonventionen sind für Benutzer und Benutzergruppen festgelegt?				M 2.91
510.04	Entspricht die Vergabe von Namen für Benutzer und Benutzergruppen diesen Festlegungen?				M 2.91
510.05	Wurden der Organisationsstruktur entsprechend Benutzergruppen angelegt?				M 4.50
510.06	Wurden für Projektgruppen entsprechende Benutzergruppen angelegt?				M 4.50
510.07	Werden Benutzerkonten in globalen Gruppen zusammengefasst?				M 4.50
510.08	Erfolgt die Vergabe von Benutzerrechten und Zugriffsberechtigungen letztlich dadurch, dass die globalen Gruppen mit den Benutzerkonten Mitglied der entsprechenden lokalen Gruppen werden?				M 4.50
510.09	Werden beim Ausscheiden von Beschäftigten deren Konten sofort deaktiviert und nach einer geeigneten Übergangszeit (ca. ½ Jahr) gelöscht?				M 2.92
510.10	Wie erfährt die Systemadministration vom Ausscheiden von Beschäftigten?				M 2.92
510.11	Bestehen entsprechende schriftliche Regelungen?				M 2.92
510.11.1	Sind die entsprechenden Regelungen ausreichend?				M 2.92
510.12	Wird regelmäßig überprüft, ob Benutzerkonteninhaber noch Beschäftigte der Organisation sind?				M 2.92
510.12.1	Wie häufig finden diese Überprüfungen statt?				M 2.92
510.12.2	Wer ist für diese Prüfungen zuständig?				M 2.92
510.12.3	Wie lang ist ein Prüfungsintervall?				M 2.92

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
510.12.4	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 2.92**
510.12.5	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 2.92**
510.12.6	**Werden diese Prüfungen dokumentiert?**				**M 2.92**
510.13	**Wird regelmäßig kontrolliert, ob die Zuordnung der Benutzer zu den Gruppen und die Mitgliedschaft der globalen Gruppen in lokalen Gruppen noch mit den aktuellen Aufgaben der Benutzer bzw. Organisationseinheiten übereinstimmt?**				**M 2.92** **M 4.50**
510.13.1	**Wer ist für diese Prüfungen zuständig?**				**M 2.92** **M 4.50**
510.13.2	**Wie lang ist ein Prüfungsintervall?**				**M 2.92** **M 4.50**
510.13.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 2.92** **M 4.50**
510.13.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 2.92** **M 4.50**
510.13.5	**Werden diese Prüfungen dokumentiert?**				**M 4.50**
510.14	**Welche Benutzerkonten sind Mitglied in den folgenden privilegierten Gruppen?** **Administratoren** **Domänen-Admins** **Hauptbenutzer (nur auf Workstations)** **Konten-Operatoren** **Sicherungs-Operatoren** **Server-Operatoren**				**M 4.50**
510.14.1	**Ist schriftlich festgelegt, wer auf dem betrachteten System Administratorrechte ausüben darf?**				**M 2.91**
510.14.2	**Welche Unterverwalter haben Zugang zu privilegierten Benutzerkonten, d.h. zu Benutzerkonten, die Mitglied der Gruppe „Hauptbenutzer“ sind?**				**M 4.50**
510.14.3	**Ist die jeweilige Mitgliedschaft in den privilegierten Gruppen jeweils zwingend zur Erledigung der übertragenen Aufgabe erforderlich?**				**M 4.50**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
510.14.4	**Entspricht die Mitgliedschaft in den privilegierten Gruppen den schriftlichen Vorgaben?**				**M 4.50**
510.14.5	**Verfügen Mitarbeiter, deren Benutzerkonto Mitglied in einer der privilegierten Gruppen ist, noch über ein Benutzerkonto, das lediglich Mitglied in der Gruppe der Domänen-Benutzer bzw. Benutzer und ggf. Mitglied in freidefinierten Gruppen ist?**				**M 4.50**
510.14.6	**Werden Konten, die der Gruppe der Administratoren bzw. Domänen-Admins angehören, zum Arbeiten nur benutzt, wenn zwingend die volle Kontrolle über das System erforderlich ist?**				**M 4.50**
510.14.7	**Werden Routinearbeiten zur Steuerung des Domänencontrollers unter einem Benutzerkonto durchgeführt, das lediglich Mitglied in der Gruppe der Server-Operatoren ist?**				**M 4.50**
510.14.8	**Werden Datensicherungen insbesondere auf Servern unter einem Benutzerkonto ausgeführt, das lediglich Mitglied der Gruppe der Sicherungs-Operatoren ist?**				**M 4.50**
510.14.9	**Gehört der Gruppe „Replikations-Operator“ ausschließlich ein Konto an, das zum Anmelden des Replikationsdienstes der Arbeitsstation dient?**				**M 4.50**
510.14.9.1	**Verfügt dieses Konto weder über das Recht „Lokale Anmeldung“ noch über das Recht „Zugriff auf diesen Computer vom Netz“?**				**M 4.50**
510.15	**Gehören Benutzer, die keine weitergehenden Benutzerrechte benötigen, ausschließlich den Gruppen „Benutzer“ bzw. „Domänenbenutzer“ und freidefinierten Benutzergruppen an?**				**M 4.50**
510.16	**Für alle Windows NT Systeme:**				
510.16.1	**Ist das vordefinierte Administratorkonto auf einen nicht leicht erratbaren Namen umbenannt worden?**				**M 4.77**
510.16.2	**Wurde das vordefinierte Administratorkonto bei der Installation mit einem sicheren Passwort versehen, dass möglichst 14 Zeichen lang ist?**				**M 4.77**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
510.16.3	**Wurde das Passwort für das vordefinierte Administratorkonto sicher hinterlegt?**				**M 4.77**
510.16.4	**Ist sichergestellt, dass zur Administration des Systems nicht das vordefinierte Administratorkonto sondern Benutzerkonten verwendet werden, die der Gruppe „Administratoren“ bzw. „Domänen-Admins“ hinzugefügt wurden?**				**M 4.77**
510.16.5	**Ist sichergestellt, dass für die Konten, die nach der Installation den Gruppen „Administratoren“ bzw. „Domänen-Admins“ hinzugefügt wurden, sichere Passwörter (s. M 2.11 Regelung des Passwortgebrauchs) benutzt werden, die mindestens 8 Zeichen lang sind?**				**M 4.77**
510.16.6	**Wurde nach der Installation ein neues Konto mit dem Namen Administrator angelegt?**				**M 4.77**
510.16.6.1	**Wurde dieses Konto mit einem Passwort versehen?**				**M 4.77**
510.16.6.2	**Wurde dieses Konto deaktiviert?**				**M 4.77**
510.16.6.3	**Gehört dieses Konto lediglich der Gruppe „Gäste“ an?**				**M 4.77**
510.16.6.4	**Wird das Sicherheitsprotokoll regelmäßig auf Anmeldeversuche mit Konten, die über Administratorrechte verfügen, überprüft?**				**M 4.77**
	Ende {Für alle Windows NT Systeme:}				
510.17	**Zusätzlich auf Windows NT Servern (einschließlich Domänencontrollern):**				
510.17.1	**Sind die Administratorkonten auf den verschiedenen Servern mit unterschiedlichen Passwörtern versehen?**				**M 4.77**
510.17.2	**Kann auf eine Fernadministration der Server über das Netz verzichtet werden?**				**M 4.77**
510.17.2.1	**Falls ja:**				
510.17.2.1.1	**Ist der Gruppe „Administratoren“ das Recht „Zugriff auf diesen Computer vom Netz“ entzogen?**				**M 4.77**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
510.17.2.2	**Sonst falls nein:**				
510.17.2.2.1	**Ist sichergestellt, dass eine Anmeldung über das Netz mit Benutzerkonten, die über Administrator-rechte verfügen, nur über in den Kontenrichtlinien festgelegte Rechner erfolgen kann?**				**M 4.77**
510.17.2.2.2	**Werden diese Rechner unter dem Betriebssystem Windows NT betrieben?**				**M 4.77**
510.17.2.2.3	**Sind die Rechner, über die fernadministriert wird, in gesicherten Bereichen aufgestellt?**				**M 4.77**
	Ende {Kann auf eine Fernadministration der Server über das Netz verzichtet werden?}				
	Ende {Zusätzlich auf Windows NT Servern}				
510.18	**Zusätzlich auf Domänencontrollern:**				
510.18.1	**Wurde das vordefinierte Administratorkonto aus der Gruppe der „Domänen-Admins“ entfernt?**				**M 4.77**
510.18.2	**Wurde das vordefinierte Administratorkonto aus der Gruppe der „Domänen-Benutzer“ entfernt?**				**M 4.77**
510.18.2.1	**Wurden dazu dieser Gruppe sämtliche System-rechte, insbesondere das Recht „Zugriff auf diesen Computer über das Netz“ entzogen?**				**M 4.77**
510.18.2.2	**Wurde dazu das vordefinierte Administratorkonto dieser Gruppe hinzugefügt?**				**M 4.77**
510.18.2.3	**Wurde dazu diese Gruppe als primäre Gruppe des vordefinierten Administratorkontos konfiguriert?**				**M 4.77**
	Ende {Zusätzlich auf Domänencontrollern:}				
510.19	**Nur bei Windows NT Workstations:**				
510.19.1	**Wird für das Administratorkonto auf allen zum System gehörenden Windows NT Workstations das gleiche Passwort benutzt?**				**M 4.77**
510.19.1.1	**Falls ja:**				
510.19.1.1.1	**Ist dies unter Berücksichtigung des Schutzbedarfs der auf den Workstations gehaltenen Daten ver-**				**M 4.77**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	tretbar?				
	Ende {Nur bei Windows NT Workstations:}				
510.20.1	**Ist das vordefinierte Gastkonto mit einem Passwort versehen worden?**				**M 4.55**
510.20.2	**Ist das vordefinierte Gastkonto gesperrt worden?**				**M 4.55**
510.20.2.1	**Falls ja:**				
510.20.2.1.1	**Wird regelmäßig geprüft, ob die Sperre noch besteht?**				**M 4.55**
510.20.2.2	**Sonst falls das Gastkonto nicht gesperrt ist:**				
510.20.2.2.1	**Ist die Benutzung des Gastkontos zwingend erforderlich?**				**M 4.55**
510.20.2.2.2	**Wird diese Notwendigkeit regelmäßig überprüft?**				**M 4.55**
510.20.2.2.3	**Wird regelmäßig geprüft, ob die Benutzerkonten-zuordnungen zur Gruppe „Gäste“ noch aktuell sind?**				**M 4.55**
510.20.2.2.3.1	**Wer ist für diese Prüfungen zuständig?**				**M 4.55**
510.20.2.2.3.2	**Wie lang ist ein Prüfungsintervall?**				**M 4.55**
510.20.2.2.3.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 4.55**
510.20.2.2.3.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 4.55**
510.20.2.2.3.5	**Werden diese Prüfungen dokumentiert?**				**M 4.55**
	Ende {Ist das vordefinierte Gastkonto gesperrt worden?}				
510.21	**Bei Einsatz des FTP-Dienstes auf dem untersuchten System:**				**M 5.43**
510.21.2	**Ist die für die anonyme Verbindung verwendete Benutzerkennung Mitglied der Gruppe „Gäste“ und keinesfalls Mitglied der Gruppe „Benutzer“ oder einer privilegierten Gruppe?**				**M 5.43**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	Ende {Bei Einsatz des FTP-Dienstes auf dem untersuchten System:}				

520 Kontenrichtlinien

520.01	**Welche Benutzerkonten-Richtlinien gibt es in der betrachteten Organisation?**				**M 2.91** **M 4.48**
520.02	**Sind diese Richtlinien dokumentiert?**				**M 2.91** **M 4.48**
520.03	**Entsprechen die vorhandenen Richtlinien und ihre Umsetzung folgenden Vorgaben?**				
520.03.1	**Ist, z.B. durch entsprechende Anweisung, sichergestellt, dass durch den Systemadministrator für jedes neu angelegte Benutzerkonto ein Passwort vergeben wird?**			**###Nummerierung?** **Was ist damit gemeint??**	**M 2.91** **M 4.48**
520.03.2	**Wird die immer gleiche Wahl des Anfangspasswortes ebenso vermieden, wie die Gleichsetzung von Benutzernamen und Passwort?**				**M 2.91** **M 4.48**
520.03.3	**Wird bei der Neuanlage normaler Benutzerkonten die Option „Benutzer muss Kennwort bei der nächsten Anmeldung ändern“ regelmäßig gewählt?**				**M 2.91** **M 4.48**
520.03.4	**Ist darauf verzichtet worden, Benutzerkonten mit der Option „Kennwort läuft nie ab“ einzurichten?**				**M 2.91** **M 4.48**
520.03.4.1	**Falls nein:**				
520.03.4.1.1	**Handelt es sich bei diesen Benutzerkonten ausschließlich um Benutzerkonten, denen mit Hilfe der Systemsteuerungsoption „Dienste“ ein Dienst zugewiesen wird?**				**M 2.91** **M 4.48**
	Ende {Ist darauf verzichtet worden, Benutzerkonten mit der Option „Kennwort läuft nie ab“ einzurichten?}				
520.03.5	**Ist das maximale Kennwortalter mit 90 Tagen festgelegt?**				**M 2.91** **M 4.48**
520.03.6	**Ist die minimale Kennwortlänge mit 6 Zeichen festgelegt?**				**M 2.91** **M 4.48**
520.03.7	**Wird beim minimalen Kennwortalter ein Wechsel erst nach 1 Tag zugelassen?**				**M 2.91** **M 4.48**
510.03.8	**Werden in der Passworthistorie mindestens die letzten 6 Passwörter gespeichert?**				**M 2.91** **M 4.48**
520.03.9	**Werden Konten nach 3 ungültigen Passworteingaben gesperrt?**				**M 2.91** **M 4.48**

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
520.03.10	**Erfolgt die Rücksetzung des Zählers für eine Passwortfalscheingabe erst nach minimal 30 Minuten?**				**M 2.91 M 4.48**
520.03.11	**Werden Konten, bei denen die maximale Anzahl an Passwortfalscheingaben überschritten wurde, gesperrt, bis ein Administrator die Sperre aufhebt?**				**M 2.91 M 4.48**
520.03.12	**Werden die Einstellungen im Benutzermanager – Richtlinien für Konten – regelmäßig kontrolliert?**				**M 2.91 M 4.48**
520.03.12.1	**Wer ist für diese Prüfungen zuständig?**				**M 2.91 M 4.48**
520.03.122	**Wie lang ist ein Prüfungsintervall?**				**M 2.91 M 4.48**
520.03.12.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 2.91 M 4.48**
520.03.12.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 2.91 M 4.48**
520.03.12.5	**Wurden diese Prüfungen dokumentiert?**				**M 2.91 M 4.48**
520.03.13	**Falls RAS zum Einsatz kommt:**				
520.03.13.1	**Ist schriftlich festgelegt, welche Benutzer die RAS-Funktionen benutzen dürfen?**				**M 5.41**
520.03.13.2	**Ist nur dem absolut notwendigen Personenkreis die Berechtigung erteilt worden, RAS-Funktionen zu benutzen?**				**M 5.41**
520.03.13.3	**Wird die Liste der für den RAS-Zugriff autorisierten Benutzer regelmäßig überprüft?**				**M 5.41**
520.03.13.3.1	**Wer ist für diese Prüfungen zuständig?**				**M 5.41**
520.03.13.3.2	**Wie lang ist ein Prüfungsintervall?**				**M 5.41**
520.03.13.3.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 5.41**
520.03.13.3.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 5.41**
520.03.13.3.5	**Werden diese Prüfungen dokumentiert?**				**M 5.41**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
520.03.13.4	**Entspricht die Vergabe der RAS-Berechtigungen den schriftlichen Vorgaben?**				**M 5.41**
520.03.13.5	**Werden regelmäßig die entsprechenden Einstel-lungen im Benutzermanager mit den Eintragungen in der Liste unter 520.03.13.1 verglichen?**				**M 5.41**
520.03.13.5.1	**Wer ist für diese Prüfungen zuständig?**				**M 5.41**
520.03.13.5.2	**Wie lang ist ein Prüfungsintervall?**				**M 5.41**
520.03.13.5.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 5.41**
520.03.13.5.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 5.41**
520.03.13.5.5	**Werden diese Prüfungen dokumentiert?**				**M 5.41**
	Ende {Falls RAS zum Einsatz kommt:}				

530 Benutzerrechte

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
530.01	Ist die Vergabe von Systemrechten – gemessen am Schutzbedarf – sinnvoll festgelegt?				M 2.91 M 4.50
530.02	Werden Benutzerrechte ausschließlich an lokale Gruppen und nicht an einzelne Benutzer vergeben?				M 4.50
530.03	Wird regelmäßig überprüft, ob die Zuweisung von Sonderrechten an Gruppen oder einzelne Benutzer noch dem aktuellen Stand entspricht?				M 2.92
530.03.1	Wer ist für diese Prüfungen zuständig?				M 2.92
530.03.2	Wie lang ist ein Prüfungsintervall?				M 2.92
530.03.3	Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?				M 2.92
530.03.4	Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?				M 2.92
530.03.5	Werden diese Prüfungen dokumentiert?				M 2.92
530.04	Wird bei der Veränderung der Gruppenmitgliedschaft eines Benutzers überprüft, ob dies zu einer Anhäufung von Benutzerrechten führt?				M 2.92
530.05	Ist der Gruppe „Jeder“ das Recht „System herunterfahren“ und das Recht „Lokale Anmeldung“ entzogen worden?				M 2.91
530.06	Ist der Gruppe „Gäste“ das Recht „Lokale Anmeldung“ entzogen worden?				M 2.91
530.07	Falls es sich um einen Server handelt:				
530.07.1	Wird das Benutzerrecht „Lokale Anmeldung“ nur für Mitglieder der Gruppen vergeben, die dieses Recht zwingend benötigen (z. B. Administratoren, Domänen-Admins, Server-Operatoren und Sicherungs-Operatoren)?				M 4.49
530.07.1.1	Wird die Vergabe dieses Benutzerrechtes regelmäßig überprüft?				M 4.49

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
530.07.1.2	**Wer ist für diese Prüfungen zuständig?**				**M 4.49**
530.07.1.2.1	**Wie lang ist ein Prüfungsintervall?**				**M 4.49**
530.07.1.2.2	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 4.49**
530.07.1.2.3	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 4.49**
530.07.1.2.4	**Werden diese Prüfungen dokumentiert?**				**M 4.49**
	Ende {Falls es sich um einen Server handelt:}				

540 Überwachungsrichtlinien (Protokollierung)

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
540.01	Welche Vorgaben für die Protokollierung gibt es?				M 4.54
540.02	Sind die Vorgaben für die Protokollierung schriftlich dokumentiert?				M 4.54
540.03	Ist die Protokollierung auf das notwendige Minimum beschränkt?				
540.04	Wer ist für die Auswertung der Protokolle zuständig?				M 4.54
540.04.1	In welchem Rhythmus werden die Protokolle ausgewertet?				M 4.54
540.04.2	Entspricht die Länge des Auswertungsintervalls den Festlegungen in der Sicherheitsstrategie?				M 4.54
540.04.3	Entspricht die Länge des Auswertungsintervalls dem festgestellten Schutzbedarf?				M 4.54
540.04.4	Werden die Auswertungen dokumentiert?				M 4.54
540.05	Wie wird auf sicherheitskritische Protokolleinträge reagiert?				M 4.54
540.05.1	Gibt es entsprechende schriftliche Festlegungen				M 4.54
540.05.2	Werden die Ursachen sicherheitskritischer Protokolleinträge analysiert und entsprechende Konsequenzen abgeleitet und umgesetzt?				M 4.54
540.06	Sind die Vorgaben für die Protokollierung im Benutzermanager bzw. im Benutzermanager für Domänen wie folgt eingestellt? **Bereich — Erfolg — Fehler** An- und Abmelden — X — X Datei- und Objektzugriffe — - — X Verwenden von Benutzerrechten — - — X Benutzer- u. Gruppenverwaltung — X — X Sicherheitsrichtlinienänderung — X — X Neustarten, Herunterfahren u. System- — X — X Prozeßverfolgung-				M 4.54

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
540.07	**Reichen diese Festlegungen unter Berücksichtigung des Schutzbedarfes aus ? Hinweis: Bei hohem oder sehr hohem Schutzbedarf sollten auch erfolgreiche Zugriffe auf besonders schutzwürdige Dateien und Objekte protokolliert werden.**				**M 4.54**
540.08	**Wird in Abhängigkeit vom Schutzbedarf eine Protokollierung von Zugriffen und Zugriffsversuchen auf die Registrierung oder auf Schlüssel bzw. Teilschlüssel der Registrierung für notwendig erachtet?**				**M 4.54**
540.08.1	**Falls ja:**				
540.08.1.1	**Ist bei den Vorgaben für die Protokollierung im Benutzermanager / Benutzermanager für Domänen die Protokollierung für Datei- und Objektzugriffe im Erfolgsfall zugelassen?**				**M 4.54**
	Ende {Wird in Abhängigkeit vom Schutzbedarf eine Protokollierung von Zugriffen und Zugriffsversuchen auf die Registrierung oder auf Schlüssel bzw. Teilschlüssel der Registrierung für notwendig erachtet?}				
540.09	**Ist die Größe der Protokolldatei ausreichend dimensioniert?**				**M 4.54**
540.09.1	**Ist durch Wahl der Größe der Protokolldatei sichergestellt, dass die Datei innerhalb des Zeitraumes zwischen zwei Überprüfungen zu maximal 30% gefüllt wird?**				**M 4.54**
540.09.2	**Wird die Option „Ereignisse nie löschen“ nur dann benutzt, wenn dies aufgrund des hohen Schutzbedarfes zwingend erforderlich ist?**				**M 4.54**
540.09.3	**Konnte bisher ausgeschlossen werden, dass eine vollgelaufene Protokolldatei zum Stillstand des Rechners führte?**				**M 4.54**
540.09.4	**Wird die Benutzung privilegierter Konten anhand des Sicherheitsprotokolls regelmäßig überprüft?**				**M 2.92**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
540.09.5	**Wird das Protokoll regelmäßig auf fehlerhafte Anmeldeversuche überprüft?**				**M 2.92**
540.05.5.1	**Wer ist für diese Prüfungen zuständig?**				**M 2.92**
540.05.5.2	**Wie lang ist ein Prüfungsintervall?**				**M 2.92**
540.09.5.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 2.92**
540.05.5.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 2.92**
540.09.5.5	**Werden diese Prüfungen dokumentiert?**				**M 2.92**
540.10	**Falls Zugriffe auf Dateien protokolliert werden:**				
540.10.1	**Wird das Protokoll auf das Vorliegen fehlgeschlagener Zugriffsversuche mindestens wöchentlich kontrolliert?**				**M 2.92**
540.10.1.1	**Wer ist für diese Prüfungen zuständig?**				**M 2.92**
540.10.1.2	**Wie lang ist das Prüfungsintervall?**				**M 2.92**
540.10.1.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 2.92**
540.10.1.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 2.92**
540.10.1.5	**Werden diese Prüfungen dokumentiert?**				**M 2.92**
540.10.2	**Welche Reaktion erfolgt auf Berechtigungsverstöße?**				**M 2.92**
	Ende {Falls Zugriffe auf Dateien protokolliert werden:}				
540.11	**Falls Zugriffe auf die Registrierung protokolliert werden:**				
540.11.1	**Wird das Protokoll auf das Vorliegen fehlgeschlagener Zugriffsversuche mindestens wöchentlich kontrolliert?**				**M 2.92**
540.11.1.1	**Wer ist für diese Prüfungen zuständig?**				**M 2.92**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
540.11.1.2	**Wie lang ist das Prüfungsintervall?**				**M 2.92**
540.11.1.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 2.92**
54011.1.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 2.92**
540.11.1.5	**Werden diese Prüfungen dokumentiert?**				**M 2.92**
540.11.2	**Welche Reaktion erfolgt auf Berechtigungsverstöße?**				**M 2.92**
540.31	**Ende {Falls Zugriffe auf die Registrierung protokolliert werden:}**				

550 Eingetragene Vertrauensstellungen

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
550.01	**Welche Vertrauensstellungen sind für das betrachtete System in der Sicherheitsstrategie vorgesehen?**				**M 2.93**
550.02	**Entsprechen die eingetragenen Vertrauensstellungen den Vorgaben der Sicherheitsstrategie?**				**M 2.93**
550.03	**Wird regelmäßig überprüft, ob die Eintragungen noch mit den Vorgaben der Sicherheitsstrategie übereinstimmen?**				**M 2.93**
550.03.1	**Wer ist für diese Prüfungen zuständig?**				**M 2.93**
550.03.2	**Wie lang ist ein Prüfungsintervall?**				**M 2.93**
550.03.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 2.93**
550.03.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 2.93**
550.03.5	**Werden diese Prüfungen dokumentiert?**				**M 2.93**

Befragte Person: Geprüft von: Datum:

560 Benutzerprofile

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
560.01	Welche Benutzerprofile sieht das Sicherheitskonzept für das untersuchte System vor?				M 4.51
560.02	Welche Einschränkungen der Nutzungsmöglichkeiten von Windows NT für „normale“ Benutzer sind in der Organisation vorgesehen?				M 4.51
560.03	Sind diese Einschränkungen schriftlich dokumentiert?				M 4.51
560.04	Wurden die Benutzerprofile vor Einsatz darauf getestet, ob sie weder Lücken enthalten noch die Benutzer an der Aufgabenerfüllung hindern?				M 4.51
560.05	Entsprechen die erstellten Benutzerprofile der Sicherheitspolitik der Organisation?				M 4.51
560.06	Ist der Arbeitsaufwand, der im Bereich der Systemadministration durch Umsetzung von Benutzerwünschen (Änderung der Schriftgröße...) im Zusammenhang mit Benutzerprofilen besteht, unter Berücksichtigung des Schutzbedarfs der Organisation vertretbar?				M 4.51
560.07	Findet eine regelmäßige Anpassung der Benutzerprofile an geänderte Rahmenbedingungen statt?				M 4.51
560.08	Falls das Gastkonto aktiviert ist:				
560.08.1	Ist das Gastkonto durch ein Profil auf die minimal erforderliche Funktionalität eingeschränkt?				M 4.51
	Ende {Falls das Gastkonto aktiviert ist}				
560.09	Nur Windows NT 3.51:				
560.09.1	Ist der Zugriff der Anwender auf die Programme und Programmgruppen beschränkt, die zwingend zur Erledigung der Fachaufgabe benötigt werden?				M 4.51
560.09.2	Ist den Benutzern das Verbinden bzw. Trennen von Netzwerkdruckern verboten worden (optional)?				M 4.51
560.09.3	Wird erzwungen, dass die Ausführung eines Anmeldeskriptes abgewartet wird, bevor der Programm-Manager gestartet wird?				M 4.51

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	Ende {Nur Windows NT 3.51:}				
560.10	**Nur Windows NT 4.0:**				
560.10.1	**Ist den Benutzern der Zugriff auf die Systemsteuerung entzogen?**				**M 4.51**
560.10.2	**Ist dabei auch die Steuerungsoption „Anzeige“ bzw. die Registerkarte „Bildschirmschoner“ mit einbezogen?**				**M 4.51**
560.10.3	**Sind die Programme zur Bearbeitung der Registrierung deaktiviert (System)?**				**M 4.51**
560.10.4	**Ist der Zugriff der Anwender auf die Programme beschränkt, die zwingend zur Erledigung der Fachaufgabe benötigt werden?**				**M 4.51**
	Ende {Nur Windows NT 4.0:}				

600 Ressourcenverwaltung

610 Verwaltung von Verzeichnissen und Dateien

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
610.01	**Sind Regeln festgelegt worden, nach denen Verzeichnisse eingerichtet werden?**				**M 2.91**
610.02	**Welche Namenskonventionen gelten für die Bezeichnung von Verzeichnissen?**				**M 2.91**
610.03	**Entspricht die Vergabe von Verzeichnisnamen diesen Festlegungen?**				**M 2.91**
610.04	**Sind die Namenskonventionen eindeutig?**				**M 2.91**
610.05	**Ist für Verzeichnisse, auf deren Inhalt nicht geschlossen werden soll, die Verwendung von Pseudonymen vorgesehen?**				**M 2.91**
610.06	**Welche Programmverzeichnisse sind auf dem untersuchten System angelegt worden?**				**M 4.53**
610.07	**Entspricht die Bezeichnung der Programmverzeichnisse den bestehenden Vorgaben?**				**M 4.53**
610.08	**Wurde festgelegt, ob Benutzerdaten lokal und/oder auf dem Server gespeichert werden sollen?**				**M 2.91**
610.09	**Ist diese Festlegung schlüssig dokumentiert?**				**M 2.91**

Befragte Person: Geprüft von: Datum:

620 NTFS-Berechtigungen

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
620.01	Werden Zugriffsberechtigungen ausschließlich an Gruppen und nicht an einzelne Benutzer vergeben?				M 4.50
620.02	Welche schriftlichen Vorgaben bestehen hinsichtlich der Vergabe von Zugriffsberechtigungen auf Dateien und Verzeichnisse unter Windows NT?				M 2.91 M 4.53
620.03	Sind zur Planung der Vorgaben Berechtigungsmatrizen aufgestellt worden?				M 4.53
620.04	Wurden die Zugriffsrechte für die Verzeichnisse %SystemRoot%, %SystemRoot%\SYSTEM und für weitere Programmverzeichnisse wie z. B. \MsOffice und \Programme sowie alle Unterverzeichnisse wie folgt vergeben: Benutzer(gruppe) — Zugriffsrecht SYSTEM — Vollzugriff Administratoren — Vollzugriff Benutzer — Lesen				M 4.53
620.05	Sind die für den Systemstart kritischen Dateien (\BOOT.INI, \NTDETECT.COM, \NTLDR, \AUTOEXEC.BAT und \CONFIG.SYS gegen unberechtigte Benutzung durch folgende Zugriffsrechtevergabe geschützt? Benutzer(gruppe) — Zugriffsrecht SYSTEM — Vollzugriff Administratoren — Vollzugriff Benutzer — Ausführen (X)				M 4.53 M 4.49
620.06	Sind alle ausführbaren Dateien (EXE-, COM- und BAT-Dateien) und die dynamischen Bibliotheken (DLL-Dateien) durch Vergabe folgender Zugriffsrechte geschützt? Benutzer(gruppe) — Zugriffsrecht SYSTEM — Vollzugriff				M 4.53

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	Administratoren Vollzugriff **Benutzer Lesen (RX)**				
620.07	**Sind die temporären Dateien gegen unautorisierte Einsichtnahme durch die Vergabe folgender Zugriffsberechtigungen auf das Verzeichnis %TEMP% geschützt?** **Benutzer(gruppe) Zugriffsrecht** **SYSTEM Vollzugriff** **Administratoren Vollzugriff** **Ersteller/Besitzer Ändern** **Benutzer Hinzufügen**				**M 4.53**
620.08	**Wird die Attributvergabe (Vergabe von Zugriffsberechtigungen) bei Systemdateien und der Registrierung regelmäßig überprüft?**				**M 4.53**
620.08.1	**Wer ist für diese Prüfungen zuständig?**				**M 4.53**
620.08.2	**Wie lang ist ein Prüfungsintervall?**				**M 4.53**
620.08.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 4.53**
620.08.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 4.53**
620.08.5	**Werden diese Prüfungen dokumentiert?**				**M 4.53**
620.09	**Sind die Zugriffsrechte auf das Profilverzeichnis für alle Benutzer (All Users) und auf das Verzeichnis für die Vorlage für neue Benutzer (Default User) wie folgt vergeben:** **Benutzer(gruppe) Zugriffsrecht** **SYSTEM Vollzugriff** **Administratoren Vollzugriff**				**M 4.53**
620.10	**Sind die Zugriffsrechte auf die Benutzerverzeichnisse (Basisverzeichnisse) wie folgt vergeben?** **Benutzer(gruppe) Zugriffsrecht**				**M 4.53**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	SYSTEM Vollzugriff **Betreffender Benutzer Vollzugriff**				
620.11	**Wird die Attributvergabe (Vergabe von Berechtigungen) auf die zuvor genannten Verzeichnisse und Dateien regelmäßig überprüft?**				
620.11.1	**Wer ist für diese Prüfungen zuständig?**				**M 4.53**
620.11.2	**Wie lang ist ein Prüfungsintervall?**				**M 4.53**
620.11.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 4.53**
620.11.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 4.53**
620.11.5	**Werden diese Prüfungen dokumentiert?**				**M 4.53**
620.12	**Welche Vorgaben existieren für die Vergabe von Zugriffsrechten auf Gruppen- und Projektverzeichnisse?**				**M 4.53**
620.12.1	**Sind die Zugriffsrechte auf Gruppen- und Projektverzeichnisse gemäß den bestehenden Vorgaben des Sicherheitskonzepts vergeben worden?**				**M 4.53**
620.13	**Welche Verzeichnisse enthalten sensitive Daten?**				**M 4.53**
620.13.1	**Wird regelmäßig überprüft, dass auf sensitive Daten nicht zu weitgehende Berechtigungen vergeben werden?**				**M 2.92**
620.13.2	**Wird die Attributvergabe (Vergabe von Berechtigungen) auf diese Verzeichnisse regelmäßig überprüft?**				
620.13.2.1	**Wer ist für diese Prüfungen zuständig?**				**M 4.53**
620.13.2.2	**Wie lang ist ein Prüfungsintervall?**				**M 4.53**
620.13.2.3	**Entspricht die Länge das Prüfungsintervalls den Vorgaben der Sicherheitsstrategie?**				**M 2.92** **M 4.53**
620.13.2.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 4.53**
620.13.2.5	**Werden diese Prüfungen dokumentiert?**				**M 4.53**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
620.14	**Falls Mitglieder der Gruppe „Gäste“, „Domänen-Gäste“ und „Jeder“ Zugriffsberechtigungen benötigen:**				**M 4.55**
620.14.1	**Wird regelmäßig geprüft, ob die der Gruppe „Gäste“ und „Domänen-Gäste“ erteilten Zugriffsberechtigungen noch aktuell sind?**				**M 4.55**
620.14.2	**Wird regelmäßig überprüft, ob die Gruppen „Jeder“, „Gäste“ und „Domänen-Gäste“ keinen Zugriff auf sensitive Daten haben?**				**M 2.92 M 4.55**
620.14.3	**Wird regelmäßig überprüft, ob die erteilten Zugriffsberechtigungen für diese Gruppen noch zwingend benötigt werden?**				**M 2.92 M 4.55**
620.14.3.1	**Wer ist für diese Überprüfung zuständig?**				**M 2.92 M 4.55**
620.14.3.2	**Wie lang ist ein Überprüfungsintervall?**				**M 2.92 M 4.55**
620.14.3.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 2.92 M 4.55**
620.14.3.4	**Entspricht die Länge eines Überprüfungsintervalls dem festgestellten Schutzbedarf?**				**M 2.92 M 4.55**
620.14.3.5	**Werden diese Überprüfungen dokumentiert?**				**M 2.92 M 4.55**
	Ende {Falls Mitglieder der Gruppe „Gäste“, „Domänen-Gäste“ und „Jeder“ Zugriffsberechtigungen benötigen:}				
620.15	**Bei Einsatz von Windows NT 3.51:**				
620.15.1	**Sind auf das Verzeichnis %SystemRoot%\SYSTEM32\Config und auf die darin befindlichen Dateien die Zugriffsrechte mindestens wie folgt gesetzt:** **Benutzer(gruppe) — Zugriffsrecht** **SYSTEM — Vollzugriff** **Administratoren — Vollzugriff** **Ersteller/Besitzer — Ändern**				**M 4.75 M 4.53**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	Benutzer **Anzeigen**				
620.15.2	**Sind die Zugriffsrechte auf die Unterverzeichnisse innerhalb des Verzeichnisses %SystemRoot%\SYSTEM32\Config, die <u>Benutzer-profile</u> enthalten, mindestens wie folgt vergeben?** **Benutzer(gruppe) Zugriffsrecht** **SYSTEM Vollzugriff** **Administratoren Vollzugriff** **Betreffender Benutzer Vollzugriff**				**M 4.53**
	Ende {Bei Einsatz von Windows NT 3.51:}				
620.16	**Bei Einsatz von Windows NT 4.0:**				
620.16.1	**Sind auf das Verzeichnis %SystemRoot%\SYSTEM32\Config und auf die darin befindlichen Dateien die Zugriffsrechte mindestens wie folgt gesetzt?** **Benutzer(gruppe) Zugriffsrecht** **SYSTEM Vollzugriff** **Administratoren Vollzugriff** **Ersteller/Besitzer Ändern** **Benutzer Anzeigen** **Hinweis: Sofern Gäste Zugriff auf dieses Verzeichnis zwingend benötigen, ist die Gruppe „Benutzer“ durch die Gruppe „Jeder“ auszutauschen. Dies sollte aber die absolute Ausnahme darstellen.**				**M 4.75** **M 4.53**
620.16.2	**Sind die Zugriffsrechte auf das Verzeichnis %SystemRoot%\SYSTEM32\Repair wie folgt gesetzt?** **Benutzer(gruppe) Zugriffsrecht** **SYSTEM Vollzugriff** **Administratoren Vollzugriff**				**M 4.77** **M 4.53**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
620.16.3	**Sind die Zugriffsrechte auf die Unterverzeichnisse im Verzeichnis %SystemRoot%\PROFILES wie folgt vergeben?** **Benutzer(gruppe) Zugriffsrecht** **SYSTEM Vollzugriff** **Administratoren Vollzugriff** **Betreffender Benutzer Vollzugriff**				**M 4.53**
	Ende {Bei Einsatz von Windows NT 4.0:}				
620.17	**Falls auf dem betrachteten System der DHCP-Dienst installiert ist:**				
620.17.1	**Sind die Dateien DHCP.TMP, DHCP.MDB, JET.LOG und SYSTEM.MDB gegen unautorisiertes Löschen und Verändern durch folgende Rechtevergabe geschützt?** **Benutzergruppe Zugriffsrecht** **SYSTEM Vollzugriff** **Administratoren Vollzugriff**				**M 5.42**
	Ende {Falls auf dem betrachteten System der DHCP-Dienst installiert ist:}				
620.18	**Falls auf dem betrachteten System der WINS-Dienst installiert ist:**				
620.18.1	**Sind die Dateien JET.LOG, SYSTEM.MDB, WINS.MDB und WINSTMP.MDB gegen unautorisiertes Löschen und Verändern durch die Vergabe folgender Zugriffsrechte geschützt?** **Benutzergruppe Zugriffsrecht** **SYSTEM Vollzugriff** **Administratoren Vollzugriff**				**M 5.42**
	Ende {Falls auf dem betrachteten System der WINS-Dienst installiert ist:}				
620.19	**Bei Einsatz des FTP-Dienstes auf dem untersuchten System:**				**M 5.43**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
620.19.1	**Entspricht die Vergabe der NTFS-Berechtigungen für den FTP-Dienst den Festlegungen im Sicherheitskonzept?**				**M 5.43**
	Ende {Bei Einsatz des FTP-Dienstes auf dem untersuchten System:}				

630 Freigabeberechtigungen

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
630.01	Welche Konventionen gelten für die Freigabenamen von Verzeichnissen und Druckern?				M 2.91
630.02	Entspricht die Vergabe der Freigabenamen diesen Konventionen?				M 2.91
630.03	Sind die Namenskonventionen eindeutig?				M 2.91
630.04	Ist für Freigaben, auf deren Inhalt nicht geschlossen werden soll, die Verwendung von Pseudonymen vorgesehen?				M 2.91
630.05	Werden möglichst nur auf Servern Verzeichnisse zum Netzzugriff freigegeben?				M 2.91
630.06	Welche Verzeichnisse sind auf dem betrachteten System für den Zugriff über das Netz zur Freigabe vorgesehen?				M 2.91 M 2.94
630.07	Sind die Vorgaben für Freigaben schriftlich dokumentiert?				M 2.94
630.08	Werden die Vorgaben bzw. die Freigaben regelmäßig an Veränderungen im Einsatzumfeld angepasst?				M 2.94
630.09	Entsprechen die Freigaben auf dem betrachteten System den Vorgaben?				M 2.94
630.10	Sind die Rechtestrukturen für die Vergabe von Freigabeberechtigungen dokumentiert?				M 2.94
630.11	Wurden Zugriffsberechtigungen auf Datenträgern ohne NTFS-Dateisystem besonders sorgfältig vergeben?				M 2.94
630.12	Wurde aus den Zugriffskontrolllisten die Gruppe „Jeder“ entfernt und auf Laufwerken mit dem NTFS-Dateisystem durch die Gruppe „Benutzer“ bzw. auf Laufwerken mit anderen Dateisystemen durch die berechtigten Gruppen ersetzt?				M 2.94
630.13	Wird regelmäßig kontrolliert, ob die Freigabeberechtigungen noch den Vorgaben entsprechen?				M 2.94
630.13.1	Wer ist für diese Prüfungen zuständig?				M 2.94

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
630.13.2	**Wie lang ist ein Prüfungsintervall?**				**M 2.94**
630.13.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 2.94**
630.13.4	**Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?**				**M 2.94**
630.13.5	**Werden diese Prüfungen dokumentiert?**				**M 2.94**
630.14	**Sofern auf das betrachtete System Zugriffe von DOS-PCs (einschließlich Windows 3.x und Windows 95) erfolgen:**				
630.14.1	**Sind auf dem betrachteten Windows NT System die Zugriffsberechtigungen auf freigegebene Verzeichnisse, auf die auch DOS-PCs Zugriff haben, so restriktiv wie möglich eingestellt?**				**M 5.40**
630.14.2	**Wird auf solche Verzeichnisse möglichst nur lesender Zugriff gewährt?**				**M 5.40**
	Ende {Sofern auf das betrachtete System Zugriffe von DOS-PCs (einschließlich Windows 3.x und Windows 95) erfolgen:}				

640 Datei- und Verzeichnisüberwachung

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
640.01	**Welche sensiblen Datenbereiche sind auf dem betrachteten System vorhanden?**				**M 4.54**
640.02	**Werden die Datei- und Objektzugriffe auf diese sensiblen Datenbereiche zumindest im Fehlerfall protokolliert?**				**M 4.54**
640.03	**Entsprechen die Einstellungen zur Zugriffsprotokollierung den schriftlichen Festlegungen?**				**M 4.54**
640.04	**Reicht unter Berücksichtigung des Schutzbedarfs der Daten die Zugriffsprotokollierung im Fehlerfall aus?**				**M 4.54**

Befragte Person: Geprüft von: Datum:

700 Registrierung

710 Eingetragene Schlüssel / Teilschlüssel / Werte

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
710.01	Wird die Anzeige des letzten Benutzers durch den Eintrag „DontDisplayLastUserName“ im Schlüssel „Software\Microsoft\WindowsNT\CurrentVersion\Winlogon“ im Bereich „HKEY_LOCAL_MACHINE“ der Registrierung mit dem Wert REG_SZ=“1“ verhindert?				M 4.55
710.02	Sind entsprechende Eingaben in die Einträge „LegalNoticeCaption“ und „LegalNoticeText“ im Schlüssel „Software\Microsoft\WindowsNT\CurrentVersion\Winlogon“ im Bereich „HKEY_LOCAL_MACHINE“ vorhanden, damit unbefugte Benutzer vor der Anmeldung einen entsprechenden Warnhinweis erhalten?				M 4.55
710.03	Falls Server fernadministriert werden:				
710.03.1	Wurde in der Registrierung auf den Rechnern, die der Fernadministration dienen, nach der Installation des notwendigen Service Packs und ggf. des lm-Fix (s. Frage 310.11.7.1) der Schlüssel „HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\LSA“ um den Eintrag „LMCompatibilityLevel“ vom Typ „REG_DWORD“ mit dem Wert „2“ ergänzt?				M 4.77
	Ende {Falls Server fernadministriert werden:}				
710.04	Falls das untersuchte System mit einem CD-ROM-Laufwerk ausgestattet ist:				
710.04.1	Ist nach den schriftlichen Vorgaben vorgesehen, die automatische CD-ROM-Erkennung permanent zu unterbinden?				M 4.57
710.04.1.1	Falls ja:				
710.04.1.1.1	Ist in der Registrierung der Eintrag „Autorun“ im Schlüssel				M 4.57

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	„\SYSTEM\CurrentControlSet\Services\Cdrom“ im Bereich „HKEY_LOCAL_MACHINE“ auf den Wert „REG_DWORD = 0“ gesetzt worden?				
710.04.1.2	**Sonst falls nein:**				
710.04.1.2.1	**Sind die Benutzer des Systems darüber informiert worden, dass sich die automatische CD-ROM-Erkennung für jede CD-ROM einzeln durch Drücken der Umschalt-Taste (Shift) beim Einlegen der CD-ROM verhindern lässt? Hinweis: Unter Benutzer in diesem Sinne sind nur solche Personen zu verstehen, die physikalisch Zugang zum untersuchten System haben. Dies dürften bei Servern i.d.R. nur die Administratoren/Operatoren sein.**				**M 4.57**
	Ende {Ist nach den schriftlichen Vorgaben vorgesehen, die automatische CD-ROM-Erkennung permanent zu unterbinden?}				
710.04.2	**Ist im Schlüssel „SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon“ im Bereich „HKEY_LOCAL_MACHINE“ der Eintrag „AllocateCdRoms“ mit dem Wert „REG_Zeichenfolge = 1“ vorhanden? Hinweis: Hiermit wird der Zugriff auf das CD-ROM-Laufwerk auf den gerade interaktiv eingeloggten Benutzer beschränkt. Der Typ REG_Zeichenfolge, der bei Benutzung des Programms „Regedit.exe“ angezeigt wird, entspricht dem Typ „REG_SZ“ bei Verwendung des Programms „Regedt32.exe“.**				**M 4.52**
710.04.3	**Wird die Einstellung dieser Schlüssel regelmäßig überprüft?**				**M 4.52**
710.04.3.1	**Wer ist für die Überprüfung zuständig?**				**M 4.52**
710.04.3.2	**Wie lang ist das Überprüfungsintervall?**				**M 4.52**
710.04.3.3	**Entspricht die Länge des Prüfungsintervalls den**				**M 4.52**

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	Festlegungen in der Sicherheitsstrategie?				
710.04.3.4	**Entspricht die Länge des Überprüfungsintervalls dem Schutzbedarf des Systems?**				**M 4.52**
710.04.3.5	**Werden die Prüfungen dokumentiert?**				**M 4.52**
	Ende {Falls das untersuchte System mit einem CD-ROM-Laufwerk ausgestattet ist:}				
710.05	**Falls das untersuchte System über ein Diskettenlaufwerk verfügt:**				
710.05.1	**Ist im Schlüssel „SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon“ im Bereich „HKEY_LOCAL_MACHINE“ der Eintrag „AllocateFloppies“ mit dem Wert „REG_Zeichenfolge = 1vorhanden? Hinweis: Hiermit wird der Zugriff auf das Diskettenlaufwerk auf den gerade interaktiv eingeloggten Benutzer beschränkt. Der Typ REG_Zeichenfolge, der bei Benutzung des Programms „Regedit.exe“ angezeigt wird, entspricht dem Typ „REG_SZ“ bei Verwendung des Programms „Regedt32.exe“.**				**M 4.52**
710.05.2	**Wird die Einstellung dieses Schlüssels regelmäßig überprüft?**				**M 4.52**
710.05.2.1	**Wer ist für die Überprüfung zuständig?**				**M 4.52**
710.05.2.2	**Wie lang ist das Überprüfungsintervall?**				**M 4.52**
710.05.2.3	**Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?**				**M 4.52**
710.05.2.4	**Entspricht die Länge des Überprüfungsintervalls dem Schutzbedarf des Systems?**				**M 4.52**
710.05.2.5	**Werden die Überprüfungen dokumentiert?**				**M 4.52**
	Ende {Falls das untersuchte System über ein Diskettenlaufwerk verfügt:}				
710.06	**Nur bei Einsatz von Windows NT 4.0:**				

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
710.06.1	**Ist der Eintrag „winreg“ im Schlüssel „\SYSTEM\CurrentControlSet\Control\SecurePipeServers“ im Bereich „HKEY_LOCAL_MACHINE“ auf den Wert „REG_DWORD = 1“ gesetzt?**				**M 4.75**
	Ende {Nur bei Einsatz von Windows NT 4.0:}				
710.07	**Nur bei Einsatz von Windows NT 3.51:**				
710.07.1	**Wurde der Gruppe „Jeder“ die Zugriffsberechtigung auf die Wurzel des Bereichs „HKEY_LOCAL_MACHINE“ (nicht jedoch auf die darunter liegenden Schlüssel) entzogen?**				**M 4.75**
	Ende {Nur bei Einsatz von Windows NT 3.51:}				

720 Rechtevergabe auf Schlüssel und Teilschlüssel

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
720.01	Verfügt die Gruppe „Jeder“ für folgende Teile der Registrierung nur über die Zugriffsrechte „Wert einsehen“, „Teilschlüssel auflisten“, „Benachrichtigen“ und „Zugriff lesen“: im Bereich „HKEY_LOCAL_MACHINE“ \SOFTWARE\ Windows 3.1 Migration Status (mit allen Unterschlüsseln) \SOFTWARE\Microsoft\RPC (mit allen Unterschlüsseln) \SOFTWARE\Microsoft\Windows NT\ CurrentVersion unter dem Schlüssel \SOFTWARE\Microsoft\ Windows NT\CurrentVersion\: + ProfileList + AeDebug + Compatibility + Drivers + Embedding + Fonts + FontSubstitutes + GRE_Initiales + MCI + MCI Extensions + Ports (mit allen Unterschlüsseln) + WOW (mit allen Unterschlüsseln) im Bereich „HKEY_CLASSES_ROOT": „\HKEY_CLASSES_ROOT“ (mit allen Unterschlüsseln)				M 4.75
720.02	Falls das System mit einem Rechnermikrofon ausgestattet ist:				
720.02.1	Ist durch Festlegung entsprechender Zugriffsrechte auf die entsprechenden Schlüssel der Registrierung im Bereich				M 4.40

Befragte Person: Geprüft von: Datum:

Nummer				Bemerkungen / Kommentare / Begründungen	Maß-nahme
	„HKEY_LOCAL_MACHINE\HARDWARE\“ sichergestellt, dass nur der Personenkreis das Rechnermikrofon aktivieren darf, der es aus zwingenden dienstlichen/betrieblichen Gründen benötigt?				
	Ende {Falls das System mit einem Rechnermikrofon ausgestattet ist:}				

730 Zugriffsüberwachung auf Hives und Teilschlüssel

Nummer	Frage	Ja	Nein	Bemerkungen / Kommentare / Begründungen	Maß-nahme
730.01	Falls unter Berücksichtigung des festgestellten Schutzbedarfs eine Protokollierung von Zugriffen und Zugriffsversuchen auf die Registrierung bzw. auf Schlüssel und Teilschlüssel der Registrierung für notwendig erachtet wird:				
730.01.1	Reicht es aus, lediglich Veränderungen an den Schlüsseln und Teilschlüsseln der Registrierung feststellen zu können?				M 4.54
730.01.1.1	Falls ja:				
730.01.1.1.1	Wird eine geeignete Software zur Integritätssicherung (Checksummenprogramm, Hash-Programm) eingesetzt?				M 4.54
730.01.1.2	Sonst falls nein:				
730.01.1.2.1	Werden Zugriffe und Zugriffsversuche auf die Schlüssel „HKEY_LOCAL_MACHINE“ und „HKEY_USERS“ protokolliert?				M 4.54
	Werden die Protokolle regelmäßig kontrolliert?				M 4.54
730.01.1.2.3	Wer ist für diese Prüfungen zuständig?				M 4.54
730.01.1.2.4	Wie lang ist ein Prüfungsintervall?				M 4.54
730.01.1.2.5	Entspricht die Länge des Prüfungsintervalls den Festlegungen in der Sicherheitsstrategie?				
730.01.1.2.6	Entspricht die Länge des Prüfungsintervalls dem festgestellten Schutzbedarf?				M 4.54
730.01.1.2.7	Werden diese Prüfungen dokumentiert?				M 4.54
	Ende {Reicht es aus, lediglich Veränderungen an den Schlüsseln und Teilschlüsseln der Registrierung feststellen zu können?}				
	Ende {Falls unter Berücksichtigung des festgestellten Schutzbedarfs eine Protokollierung von Zugriffen und Zugriffsversuchen auf die Registrierung bzw. auf Schlüssel und Teilschlüssel der Registrierung für notwendig erachtet wird:}				

Befragte Person: Geprüft von: Datum: