Anhang C – Benutzerrechte

(Engl. Originaltitel: Appendix C - User Rights and Privileges)

Die nachstehende Tabelle zeigt die standardmäßig zugewiesenen Benutzerrechte auf Windows 2000-Systemen und definiert deren Anwendbarkeit auf das Windows 2000-Sicherheitsziel (Security Target oder ST). Darüber hinaus werden erforderliche Änderungen und Empfehlungen genannt, die zur Einhaltung des Sicherheitsziels beachtet werden sollten.

Die Tabelle enthält die Standardbenutzerrechte, die Benutzern auf eigenständigen Windows 2000 Professional- und Windows 2000 Server-Systemen sowie auf einem Windows 2000-Domänencontroller zugewiesen sind. Darüber hinaus sind die Standardbenutzerrechte in einer Domänensicherheitsrichtlinie (standardmäßig alle „nicht definiert“) angegeben. Die Zuweisungen in der Domänensicherheitsrichtlinie setzen die Einstellungen der lokalen Sicherheitsrichtlinie für Domänenmitglieder außer Kraft. Die in der Tabelle aufgeführten „erforderlichen“ Änderungen sind erforderlich, um die Einhaltung der Sicherheitszielanforderungen zu gewährleisten.

Die Zuweisungen der Benutzerrechte finden Sie wie folgt in der grafischen Benutzeroberfläche für lokale Sicherheitsrichtlinien und Domänensicherheitsrichtlinien:

- Windows 2000 Professional:

  Verwaltung\Lokale Sicherheitsrichtlinie\Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechten

- Windows 2000 Server:

  Verwaltung\Lokale Sicherheitsrichtlinie\Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechten

- Windows 2000-Domänencontroller:

  Verwaltung\Sicherheitsrichtlinie für Domänencontroller\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechten

  Verwaltung\Sicherheitsrichtlinie für Domänen\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechten

Benutzerrechte	Beschreibung	Gruppen, denen dieses Recht auf eigenständigen Windows 2000 Professional-Systemen zugewiesen ist	Gruppen, denen dieses Recht auf eigenständigen Windows 2000 Server-Systemen zugewiesen ist	Gruppen, denen dieses Recht in der Windows 2000-Sicherheitsrichtlinie für Domänen zugewiesen ist (auf dem Domänen-controller)	Gruppen, denen dieses Recht auf Windows 2000-Domänencontrollern zugewiesen ist und/oder (Sicherheitsrichtlinie für Domänencontroller) Gründe für die Änderung	Anwendbare Sicherheitszielanforderungen
Anmelderechte						
Als Dienst anmelden (SeServiceLogonRight)	Ermöglicht es einem Sicherheitsprincipal, sich als Dienst anzumelden. Dienste können für die Ausführung unter dem Konto **LocalSystem** konfiguriert werden, das über das Recht verfügt, sich als Dienst anzumelden. Jedem Dienst, der unter einem separaten Konto ausgeführt wird, muss dieses Recht zugewiesen werden.	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** (Nicht definiert) **Empfohlene Änderung:** Keine Änderung	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	
Anmelden als Stapelverarbeitungsauftrag (SeBatchLogonRight)	Ermöglicht es einem Benutzer, sich mithilfe einer Batchwarteschlange anzumelden.	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** (Nicht definiert) **Empfohlene Änderung:** Keine Änderung	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	
Anmeldung als Batchauftrag verweigern	Verhindert, dass sich ein Benutzer oder eine Gruppe anhand einer Batchwarteschlange	**Standard:**	**Standard:**	**Standard:**	**Standard:**	

(SeDenyBatchLogonRight)	anmeldet.	Kein **Empfohlene Änderung:** Keine Änderung	Kein **Empfohlene Änderung:** Keine Änderung	(Nicht definiert) **Empfohlene Änderung:** Keine Änderung	Kein **Empfohlene Änderung:** Keine Änderung	
Anmeldung als Dienst verweigern (SeDenyServiceLogonRight)	Verhindert, dass sich ein Benutzer oder eine Gruppe als Dienst anmeldet.	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** (Nicht definiert) **Empfohlene Änderung:** Keine Änderung	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	
Auf diesen Computer vom Netzwerk aus zugreifen (SeNetworkLogonRight)	Bestimmt die Benutzer, die über das Netzwerk eine Verbindung mit dem Computer herstellen dürfen.	**Standard:** Administratoren Sicherungs-Operatoren Hauptbenutzer Benutzer Jeder **Erforderliche Änderung:** Administratoren Sicherungs-Operatoren	**Standard:** Administratoren Sicherungs-Operatoren Hauptbenutzer Benutzer Jeder **Erforderliche Änderung:** Administratoren Sicherungs-	**Standard:** (Nicht definiert) **Erforderlich:** Keine Änderung	**Standard:** Administratoren Authentifizierte Benutzer Jeder **Erforderliche Änderung:** Administratoren Authentifizierte Benutzer	Unterstützt die folgende TOE-Sicherheitsfunktions-anforderung: FIA_UAU.2.1, Authentifizierung, und FIA_UID.2, Benutzeridentifizie-rung vor jedem Vorgang. Implementiert die folgenden TOE-Sicherheitsfunktionen: Abs. 6.1.3, Identifizierung und Authentifizierung für Netzwerkanmeldunge

		Hauptbenutzer Benutzer Authentifizierte Benutzer	Operatoren Hauptbenutzer Benutzer Authentifizierte Benutzer			n. **Änderungen:** Keine Anmeldung von Gästen/anonymen Benutzern zulassen. Konten, die u. U. nicht authentifizierten/anonymen Zugriff ermöglichen, entfernen/ersetzen (falls **Gast** aus irgendwelchen Gründen aktiviert wurde). **Jeder** durch **Authentifizierte Benutzer** ersetzen.
Lokal anmelden (SeInteractiveLogonRight)	Ermöglicht es einem Benutzer, sich mithilfe der Tastatur des Computers lokal anzumelden.	**Standard:** Administratoren Sicherungs-Operatoren Hauptbenutzer Benutzer *Computername*\Gast **Erforderliche Änderung:** Administratoren	**Standard:** Administratoren Sicherungs-Operatoren Hauptbenutzer Benutzer *Computername*\Gast *Computername\TsInternetUser* ***Erforderliche***	**Standard:** (Nicht definiert) **Erforderlich:** Keine Änderung	**Standard:** Administratoren Konten-Operatoren Sicherungs-Operatoren Druck-Operatoren Server-Operatoren TsInternetUser **Erforderliche Änderung:** Administratoren	Unterstützt die folgende TOE-Sicherheitsfunktionsanforderung: FIA_UAU.2.1, Authentifizierung, und FIA_UID.2, Benutzeridentifizierung vor jedem Vorgang. Implementiert die folgenden TOE-Sicherheitsfunktionen: Abs. 6.1.3, Identifizierung und Authentifizierung für

		Sicherungs-Operatoren Hauptbenutzer Benutzer	***Änderung:*** *Administratoren* *Sicherungs-Operatoren* *Hauptbenutzer* *Benutzer*		Konten-Operatoren Sicherungs-Operatoren Druck-Operatoren Server-Operatoren	lokale Anmeldungen. **Änderungen:** Keine Anmeldung von Gästen/anonymen Benutzern zulassen. Gästekonten entfernen, da sie nicht authentifizierten/anonymen Zugriff ermöglichen. Das Konto **TsInternetUser** entfernen – Terminaldienste werden für TOE nicht implementiert.
Lokale Anmeldung verweigern (SeDenyInteractiveLogonRight)	Verhindert, dass sich ein Benutzer oder eine Gruppe mithilfe der Tastatur des Computers lokal anmeldet.	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** (Nicht definiert) **Empfohlene Änderung:** Keine Änderung	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	
Zugriff vom Netzwerk auf diesen Computer verweigern (SeDenyNetworkLogonRight)	Verhindert, dass ein Benutzer oder eine Gruppe über das Netzwerk eine Verbindung mit dem Computer herstellt.	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** (Nicht definiert) **Empfohlene Änderung:** Keine Änderung	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	
Rechte						
Ändern der Systemzeit	Ermöglicht es dem	**Standard:**	**Standard:**	**Standard:**	**Standard:**	Die

(SeSystemTimePrivilege)	Benutzer, die Zeit der internen Computeruhr einzustellen.	Administratoren, Hauptbenutzer **Erforderliche Änderung:** Keine Änderung	Administratoren, Hauptbenutzer **Erforderliche Änderung:** Keine Änderung	(Nicht definiert) **Erforderliche Änderung:** Keine Änderung	Administratoren Server-Operatoren **Erforderliche Änderung:** Keine Änderung	Standardeinstellungen unterstützen die folgenden TOE-Sicherheitsfunktionsanforderungen: FMT_SMR.1, Sicherheitsrollen; und FMT_MTD.1.1(g), Verwaltung der TSF-Zeit. Implementiert die folgenden TOE-Sicherheitsfunktionen: Abs. 6.1.4.1, Rollen, und 6.1.5.6, Zeitdienst. Kann dazu verwendet werden, autorisierten Benutzern das Recht zu gewähren, die Systemzeit einzustellen.
Anheben der Zeitplanungspriorität (SeIncreaseBasePriorityPrivilege)	Ermöglicht es einem Prozess mit Schreibzugriff auf einen anderen Prozess, die Ausführungspriorität des anderen Prozesses zu erhöhen.	**Standard**: Administratoren **Empfohlen**: Keine Änderung	**Standard**: Administratoren **Empfohlen**: Keine Änderung	**Standard**: (Nicht definiert) **Erforderliche Änderung**: Administratoren	**Standard**: Administratoren **Empfohlen**: Keine Änderung	Unterstützt die folgende TOE-Sicherheitsfunktionsanforderung: FMT_SMR.1, Sicherheitsrollen. Es gibt jedoch keine Sicherheitszielanforderung, die speziell fordert, dass diese

						Möglichkeit auf den Administrator beschränkt ist. Kann verwendet werden, um die folgenden TOE-Sicherheitsfunktionen zu unterstützen: Abs. 6.1.4.1, Rollen. Kann verwendet werden, um autorisierten Benutzern die Verwaltungsmöglichkeit zu gewähren, die Ausführungspriorität von Prozessen zu erhöhen. Ein Missbrauch dieses Rechtes kann zu einem Denial-of-Service führen, einem schwerwiegenden Sicherheitsproblem, da die Verwaltung der Prozessorquote sich auf Leistung und Verfügbarkeit auswirkt. Die Abwehr von Denial-of-Service-Angriffen ist jedoch nicht Bestandteil des Sicherheitsziels.

						Änderungen: Legen Sie die Domänenrichtlinie für dieses Recht auf **Administratoren** fest, damit eine vertrauenswürdige Verwaltung erzwungen wird.
Anheben von Quoten (SeIncreaseQuotaPrivilege)	Ermöglicht es einem Prozess mit Schreibzugriff auf einen anderen Prozess, die Prozessorquote zu erhöhen, die dem anderen Prozess zugewiesen ist. Dieses Recht ist nützlich, um das System zu optimieren, kann aber z. B. in einem Denial-of-Service-Angriff missbraucht werden.	**Standard**: Administratoren **Empfohlen**: Keine Änderung	**Standard**: Administratoren **Empfohlen**: Keine Änderung	**Standard**: (Nicht definiert) **Erforderliche Änderung**: Administratoren	**Standard**: Administratoren **Empfohlen**: Keine Änderung	Kann verwendet werden, um die folgenden TOE-Sicherheitsfunktionsanforderungen zu unterstützen: FMT_SMR.1, Sicherheitsrollen. Es gibt jedoch keine Sicherheitszielanforderung, die speziell fordert, dass diese Möglichkeit auf den Administrator beschränkt ist. Kann die folgenden TOE-Sicherheitsfunktionen unterstützen: Abs. 6.1.4.1, Rollen. Kann verwendet werden, um autorisierten

						Benutzern die Verwaltungsmöglichkeit zu gewähren, die einem Prozess zugewiesene Prozessorquote zu erhöhen. Ein Missbrauch dieses Rechtes kann zu einem Denial-of-Service führen, einem schwerwiegenden Sicherheitsproblem, da die Verwaltung der Prozessorquote sich auf Leistung und Verfügbarkeit auswirkt. Die Abwehr von Denial-of-Service-Angriffen ist jedoch nicht Bestandteil des Sicherheitsziels. **Änderungen**: Legen Sie die Domänenrichtlinie für dieses Recht auf **Administratoren** fest, damit eine vertrauenswürdige Verwaltung erzwungen wird.
Auslassen der durchsuchenden Überprüfung	Ermöglicht dem Benutzer während der Navigation in einem Objektpfad eines	**Standard:**	**Standard:**	**Standard:**	**Standard:**	

(SeChangeNotifyPrivilege)	Microsoft Windows-Dateisystems oder der Registrierung die Navigation in Ordnern, auf die der Benutzer normalerweise nicht zugreifen kann. Dieses Recht ermöglicht es dem Benutzer nicht, den Inhalt eines Ordners aufzulisten, sondern nur, die zugehörigen Verzeichnisse zu durchlaufen.	Administratoren Sicherungs-Operatoren, Hauptbenutzer Benutzer Jeder **Empfohlene Änderung:** Keine Änderung	Administratoren Sicherungs-Operatoren, Hauptbenutzer Benutzer Jeder **Empfohlene Änderung:** Keine Änderung	(Nicht definiert) **Empfohlene Änderung**: Keine Änderung	Administratoren Authentifizierte Benutzer Jeder **Empfohlene Änderung:** Keine Änderung	
Debuggen von Programmen (SeDebugPrivilege)	Ermöglicht es einem Benutzer, einen Debugger in einen beliebigen Prozess einzubinden.	**Standard:** Administratoren **Erforderlich:** Keine Änderung	**Standard:** Administratoren **Erforderlich:** Keine Änderung	**Standard:** (Nicht definiert) **Erforderlich:** Keine Änderung	**Standard:** Administratoren **Erforderlich:** Keine Änderung	Die Zuweisung dieses Rechtes verletzt die TOE-Sicherheitsfunktionsanforderungen FAU_GEN.1, Generierung von Überwachungsdaten, und FDP_ACF.1(a), Zugriffssteuerung. Dieses Recht ermöglicht Benutzern unabhängig von den ACLs den Zugriff auf Objekte. Dieses Recht kann nicht überwacht werden und sollte keinen Benutzern, auch nicht Administratoren,

						zugewiesen werden. **Änderungen:** Ändern Sie alle Standardrechtezuweisungen in **Kein**, um die Einhaltung von FAU_GEN.1 und FDP_ACF.1(a) sicherzustellen.
Einsetzen als Teil des Betriebssystems (SeTcbPrivilege)	Ermöglicht es einem Prozess, einen Benutzer zu authentifizieren, und so auf dieselben Ressourcen zuzugreifen wie ein Benutzer. Dieses Recht sollte nur von Authentifizierungsdiensten auf niedriger Ebene benötigt werden. Die Zugriffsmöglichkeiten sind nicht auf die dem Benutzer standardmäßig zugewiesenen Ressourcen beschränkt, da der aufrufende Prozess anfordern kann, dass weitere Zugriffsmöglichkeiten in das Zugriffstoken eingefügt werden. Weitaus bedeutender ist die Tatsache, dass der aufrufende Prozess ein anonymes Token erstellen kann, das beliebigen	**Standard:** Kein **Erforderlich:** Keine Änderung	**Standard:** Kein **Erforderlich:** Keine Änderung	**Standard:** (Nicht definiert) **Erforderlich:** Keine Änderung	**Standard:** Kein **Erforderlich:** Keine Änderung	Die Standardeinstellungen unterstützen die folgenden TOE-Sicherheitsfunktionsanforderungen: FPT_SEP.1.2, Domänentrennung. Ein Missbrauch dieses Rechtes kann FAU_GEN.1, Generierung von Überwachungsdaten, FAU_GEN.2, Benutzeridentitätszuordnung, und FIA_USB.1, Benutzersubjektbindung, verletzen. Implementiert die folgenden TOE-Sicherheitsfunktionen:

	Zugriff auf beliebige Ressourcen zulässt. Darüber hinaus stellt das anonyme Token keine primäre Identität für die Nachverfolgung von Ereignissen im Überwachungsprotokoll bereit. Das Konto **LocalSystem** verwendet standardmäßig dieses Recht.					Abs. 6.1.5.5, Domänentrennung. Die Verwendung dieses Rechtes durch andere Konten als **LocalSystem** kann die Sicherheitsanforderung einer Zugriffskontrolle verletzten, da die Möglichkeit der Generierung anonymer Token besteht. **Änderungen:** Legen Sie die Domänenrichtlinie auf **Kein** fest, um die Standardeinstellungen in der Domäne zu erzwingen und die Unterstützung von FPT_SEP.1.2, FAU_GEN.1, FAU_GEN.2 und FIA_USB.1 sicherzustellen.
Entfernen des Computers von der Dockingstation (SeUndockPrivilege)	Ermöglicht es dem Benutzer eines tragbaren Computers, den Computer durch Klicken auf **PC trennen** im Startmenü zu entsperren.	**Standard**: Administratoren Hauptbenutzer	**Standard**: Administratoren Hauptbenutzer	**Standard**: (Nicht definiert) **Empfohlene Änderung**:	**Standard**: Administratoren **Empfohlene Änderung**: Keine Änderung	

		Benutzer **Empfohlene Änderung**: Keine Änderung	Benutzer **Empfohlene Änderung**: Keine Änderung	Keine Änderung		
Ermöglichen, dass Computer- und Benutzerkonten für Delegierungszwecke vertraut wird (SeEnableDelegationPrivilege)	Ermöglicht es dem Benutzer, die Vertrauenseinstellung für Delegierungszwecke eines Benutzers oder Computers in Active Directory zu ändern. Der Benutzer bzw. der Computer, dem dieses Recht gewährt wird, muss außerdem über Schreibzugriff auf das Kontosteuerungsflag des Objekts verfügen.	**Standard:** Kein **Erforderlich:** Keine Änderung	**Standard:** Kein **Erforderlich:** Keine Änderung	**Standard:** (Nicht definiert) **Erforderlich:** Keine Änderung	**Standard:** Administratoren **Erforderlich:** Keine Änderung	Unterstützt die folgende TOE-Sicherheitsfunktionsanforderung: FMT_SMR.1, Sicherheitsrollen. Implementiert die folgenden TOE-Sicherheitsfunktionen: Abs. 6.1.4.1, Rollen. Kann verwendet werden, um autorisierten Benutzern die Rechte für die Vertrauenseinstellung für Delegierungszwecke eines Benutzers oder Computers in Active Directory zu gewähren. Ein Missbrauch dieses Rechtes oder der Vertrauenseinstellungen für Delegierungszwecke

						kann bei Angriffen auf das System durch "trojanische Pferde" zu einer Gefährdung des Netzwerks führen, wenn diese die Identität eingehender Clients übernehmen und die Anmeldeinformationen dieser Clients für den Zugriff auf Netzwerkressourcen verwenden. **Änderungen:** Legen Sie die Domänenrichtlinie für dieses Recht auf **Kein** fest, damit ein Schutz vor nicht autorisierten Zugriffen und Änderungen besteht.
Ersetzen eines Tokens auf Prozessebene (SeAssignPrimaryTokenPrivilege)	Ermöglicht es einem übergeordneten Prozess, das einem untergeordneten Prozess zugeordnete Zugriffstoken zu ersetzen.	**Standard**: Kein **Erforderlich**: Keine Änderung	**Standard**: Kein **Erforderlich**: Keine Änderung	**Standard**: (Nicht definiert) **Erforderlich**: Keine Änderung	**Standard**: Kein **Erforderlich**: Keine Änderung	Die Zuweisung dieses Rechtes verletzt die folgenden TOE-Sicherheitsfunktionsanforderungen: FDP_ACF.1(a), Zugriffssteuerung; FIA_USB.1, Benutzersubjektbindung; und FAU_GEN.1, Generierung von

						Überwachungsdaten. Dieses Recht kann nicht überwacht werden. **Änderungen**: Ändern Sie die Standardrechtezuweisungen der Domänensicherheitsrichtlinie in **Kein**, um die Einhaltung von FDP_ACF.1(a), FIA_USB.1 und FAU_GEN.1 in der Domäne sicherzustellen. Weisen Sie dieses Recht keinem Benutzer zu.
Erstellen einer Auslagerungsdatei (SeCreatePagefilePrivilege)	Ermöglicht es dem Benutzer, eine Auslagerungsdatei zu erstellen und deren Größe zu ändern.	**Standard:** Administratoren **Erforderlich:** Keine Änderung	**Standard:** Administratoren **Erforderlich:** Keine Änderung	**Standard:** (Nicht definiert) **Erforderlich:** Administratoren	**Standard:** Administratoren **Erforderlich:** Keine Änderung	Unterstützt die folgende TOE-Sicherheitsfunktionsanforderung: FMT_SMR.1, Sicherheitsrollen. Implementiert die folgenden TOE-Sicherheitsfunktionen: Abs. 6.1.4.1, Rollen. Kann dazu verwendet

						werden, autorisierten Benutzern das Recht zu gewähren, die Einstellungen für die Auslagerungsdatei zu ändern. **Änderung:** Legen Sie die Domänenrichtlinie für dieses Recht auf **Administratoren** fest, damit eine vertrauenswürdige Verwaltung unterstützt und vor nicht autorisierten Systemänderungen geschützt wird.
Erstellen eines Profils der Systemleistung (SeSystemProfilePrivilege)	Ermöglicht es einem Benutzer, Microsoft Windows NT- und Windows 2000-Leistungsüberwachungstools auszuführen, um die Leistung von Systemprozessen zu überwachen.	**Standard**: Administratoren **Erforderlich**: Keine Änderung	**Standard**: Administratoren **Erforderlich**: Keine Änderung	**Standard**: (Nicht definiert) **Erforderliche Änderung**: Administratoren	**Standard**: Administratoren **Erforderlich**: Keine Änderung	Unterstützt die folgende TOE-Sicherheitsfunktionsanforderung: FMT_SMR.1, Sicherheitsrollen Unterstützt die folgenden TOE-Sicherheitsfunktionen: Abs. 6.1.4.1, Rollen, und Abs. 6.1.5.1, Systemintegrität. Kann verwendet werden, um

						autorisierten Benutzern die Verwaltungsmöglichkeit zu gewähren, eine Leistungsdiagnose von Systemprozessen auszuführen. **Änderungen**: Legen Sie die Domänenrichtlinie für dieses Recht auf **Administratoren** fest, damit eine vertrauenswürdige Verwaltung unterstützt wird.
Erstellen eines Profils für einen Einzelprozess (SeProfileSingleProcessPrivilege)	Ermöglicht es einem Benutzer, Microsoft Windows NT- und Windows 2000-Leistungsüberwachungstools auszuführen, um die Leistung von Nicht-Systemprozessen zu überwachen.	**Standard**: Administratoren Hauptbenutzer **Empfohlene Änderung**: Keine Änderung	**Standard**: Administratoren Hauptbenutzer **Empfohlene Änderung**: Keine Änderung	**Standard**: (Nicht definiert) **Empfohlene Änderung**: Keine Änderung	**Standard**: Administratoren **Empfohlene Änderung**: Keine Änderung	Kann verwendet werden, um die folgenden TOE-Sicherheitsfunktionsanforderungen zu unterstützen: FMT_SMR.1, Sicherheitsrollen. Kann verwendet werden, um die folgenden TOE-Sicherheitsfunktionen zu unterstützen: Abs. 6.1.4.1, Rollen. Kann verwendet werden, um

						autorisierten Benutzern die Verwaltungsmöglichkeit zu gewähren, eine Leistungsdiagnose von Nicht-Systemprozessen auszuführen. Das Verhindern der Möglichkeit durch dieses Recht ist jedoch kein ausdrückliches Sicherheitsziel.
Erstellen eines Tokenobjekts (SeCreateTokenPrivilege)	Ermöglicht es einem Prozess, ein Zugriffstoken zu erstellen, indem **NtCreateToken()** oder andere API-Funktionen zum Erstellen von Token aufgerufen werden.	**Standard:** Kein **Erforderliche Änderung:** Keine Änderung	**Standard:** Kein **Erforderliche Änderung:** Keine Änderung	**Standard:** (Nicht definiert) **Erforderlich:** Kein	**Standard:** Kein **Erforderlich:** Keine Änderung	Die Standardeinstellungen unterstützen die folgenden TOE-Sicherheitsfunktionsanforderungen: FPT_SEP.1.2, Domänentrennung. Implementiert die folgenden TOE-Sicherheitsfunktionen: Abs. 6.1.5.5, Domänentrennung. Die Verwendung dieses Rechtes kann nicht überwacht werden. Ein Missbrauch dieses

						Rechtes kann zu einer Verletzung von FIA_USB.1, Benutzersubjektbindung, und FAU_GEN.1, Generierung von Überwachungsdaten, führen. **Änderung:** Legen Sie die Domänenrichtlinie für dieses Recht auf **Kein** fest, um die Standardeinstellungen in der Domäne zu erzwingen und die Unterstützung von FPT_SEP.1.2 sicherzustellen. Verwenden Sie das Konto **LocalSystem** (das bereits über dieses Recht verfügt), wenn ein Prozess dieses Recht benötigt, anstatt ein eigenes Konto zu erstellen und ihm dieses Recht zuzuweisen.
Erstellen von dauerhaft freigegebenen Objekten (SeCreatePermanentPrivilege)	Ermöglicht es einem Prozess, im Windows 2000-Objekt-Manager ein Verzeichnisobjekt zu erstellen. Dieses Recht ist	**Standard:** Kein **Empfohlene**	**Standard:** Kein **Empfohlene**	**Standard:** (Nicht definiert) **Empfohlene**	**Standard:** Kein	

	für Kernelmoduskomponenten nützlich, die den Windows 2000-Objektnamespace erweitern. Komponenten, die im Kernelmodus ausgeführt werden, verfügen bereits über dieses Recht, sodass es nicht zugewiesen werden muss.	**Änderung:** Keine Änderung	**Änderung:** Keine Änderung	**Änderung:** Keine Änderung	**Empfohlene Änderung:** Keine Änderung	
Erzwingen des Herunterfahrens von einem Remotesystem aus (SeRemoteShutdownPrivilege)	Ermöglicht es einem Benutzer, einen Computer von einem Remotestandort im Netzwerk aus herunterzufahren.	**Standard:** Administratoren **Empfohlene Änderung:** Keine Änderung	**Standard:** Administratoren **Empfohlene Änderung:** Keine Änderung	**Standard:** (Nicht definiert) **Empfohlene Änderung:** Administratoren	**Standard:** Administratoren Server-Operatoren **Empfohlene Änderung:** Keine Änderung	
Generieren von Sicherheitsüberwachungen (SeAuditPrivilege)	Ermöglicht es einem Prozess, Einträge im Sicherheitsprotokoll zu generieren. Im Sicherheitsprotokoll werden nicht autorisierte Systemzugriffe und andere sicherheitsrelevante Aktivitäten protokolliert.	**Standard:** Kein **Erforderlich**: Keine Änderung	**Standard:** Kein **Erforderlich**: Keine Änderung	**Standard:** (Nicht definiert) **Erforderlich**: Keine Änderung	**Standard:** Kein **Erforderlich**: Keine Änderung	Unterstützt über das Konto **LocalSystem** die folgenden TOE-Sicherheitsanforderungen: FAU_GEN.1.1, Generierung von Überwachungsdaten. Wenn dieses Recht Benutzern gewährt wird, können in das Überwachungsprotokoll Überwachungseinträge

						eingefügt werden, die nicht von TFS generiert wurden. Die Verwendung dieses Rechtes kann nicht überwacht werden. **Änderungen**: Legen Sie die Domänenrichtlinie für dieses Recht auf **Kein** fest. Dieses Recht sollte keinen Benutzern, auch nicht Administratoren, gewährt werden.
Herunterfahren des Systems (SeShutdownPrivilege)	Ermöglicht es einem Benutzer, den lokalen Computer herunterzufahren.	**Standard:** Administratoren Sicherungs-Operatoren Hauptbenutzer Benutzer **Empfohlene Änderung:** Administratoren Sicherungs-Operatoren Hauptbenutzer	**Standard:** Administratoren Sicherungs-Operatoren Hauptbenutzer **Empfohlene Änderung:** Administratoren Sicherungs-Operatoren Hauptbenutzer	**Standard:** (Nicht definiert) **Empfohlene Änderung:** Keine Änderung	**Standard:** Administratoren Konten-Operatoren Sicherungs-Operatoren Server-Operatoren Druck-Operatoren **Empfohlene Änderung:** Keine Änderung	

		Authentifizierte Benutzer	Authentifizierte Benutzer			
Hinzufügen von Arbeitsstationen zur Domäne (SeMachineAccountPrivilege)	Ermöglicht es einem Benutzer, einen Computer zu einer bestimmten Domäne hinzuzufügen. Damit das Recht effektiv wird, muss es dem Benutzer als Teil der lokalen Sicherheitsrichtlinie für Domänencontroller in der Domäne zugewiesen werden. Ein Benutzer mit diesem Recht kann bis zu 10 Arbeitsstationen zur Domäne hinzufügen. In Windows 2000 wird das Verhalten dieses Rechtes durch die Berechtigung zum Erstellen von Computerobjekten für Organisationseinheiten und durch den Standardcontainer **Computer** in Active Directory dupliziert. Benutzer mit der Berechtigung zum Erstellen von Computerobjekten können eine unbegrenzte Anzahl von Computern zu der Domäne hinzufügen.	**Standard:** Kein **Erforderlich:** Keine Änderung	**Standard:** Kein **Erforderlich:** Keine Änderung	**Standard:** (Nicht definiert) **Erforderlich:** Keine Änderung	**Standard:** Authentifizierte Benutzer **Erforderliche Änderung:** Domänen-Admins	Unterstützt die folgende TOE-Sicherheitsfunktionsanforderung: FMT_SMR.1, Sicherheitsrollen. Implementiert die folgenden TOE-Sicherheitsfunktionen: Abs 6.1.4.1, Sicherheitsverwaltungsfunktionen, in dem die Domänenverwaltungsfunktion beschrieben ist, mit der ein autorisierter Administrator Computer zu einer Domäne hinzufügen und daraus entfernen kann. Abs. 6.1.4.1, Rollen. Kann dazu verwendet werden, autorisierten Benutzern das Recht zu gewähren, Computer zur Domäne hinzuzufügen und daraus zu entfernen.

						Änderungen: Ändern Sie die Standardeinstellung in der Sicherheitsrichtlinie für Domänencontroller von **Authentifizierte Benutzer** in **Domänen-Admins**, um die vertrauenswürdige Verwaltung und Konfigurationskontrolle der Domäneninfrastruktur sicherzustellen.
Laden und Entfernen von Gerätetreibern (SeLoadDriverPrivilege)	Ermöglicht es einem Benutzer, Plug & Play-Gerätetreiber zu installieren und zu deinstallieren. Dieses Recht betrifft keine nicht Plug & Play-fähigen Gerätetreiber. Diese Gerätetreiber können nur von Administratoren installiert werden. Beachten Sie, dass bei Gerätetreibern, die als vertrauenswürdige (hoch privilegierte) Prozesse ausgeführt werden, ein Benutzer dieses Recht missbrauchen kann, um böswillige Programme installiert werden, die Ressourcen zerstören	**Standard**: Administratoren **Erforderlich**: Keine Änderung	**Standard**: Administratoren **Erforderlich**: Keine Änderung	**Standard**: (Nicht definiert) **Erforderliche Änderung**: Administratoren	**Standard**: Administratoren **Erforderlich**: Keine Änderung	Unterstützt die folgende TOE-Sicherheitsfunktionsanforderung: FMT_SMR.1, Sicherheitsrollen. Implementiert die folgenden TOE-Sicherheitsfunktionen: Abs. 6.1.4.1, Rollen. Kann verwendet werden, um autorisierten Benutzern die Verwaltungsmöglichkeit zu gewähren, Gerätetreiber zu

	können.					installieren und zu konfigurieren. **Änderungen**: Legen Sie die Domänenrichtlinie für dieses Recht auf **Administratoren** fest, damit eine vertrauenswürdige Verwaltung unterstützt wird.
Read unsolicited data from a terminal device (Nicht angeforderte Daten von einem Terminalgerät lesen) (SeUnsolicitedInputPrivilege)	Erforderlich, um nicht angeforderte Daten von einem Terminalgerät zu lesen. Dieses Recht ist veraltet und wird nicht verwendet. Es hat keine Auswirkung auf das System.	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	
Sichern von Dateien und Verzeichnissen (SeBackupPrivilege)	Ermöglicht es dem Benutzer, die Datei- und Verzeichnisberechtigungen zum Sichern des Systems zu umgehen. Das Recht wird nur aktiviert, wenn der Zugriffsversuch der Anwendung über die Schnittstelle der NTFS-Sicherungsanwendung erfolgt. Andernfalls gelten die normalen Datei- und Verzeichnisberechtigungen.	**Standard:** Administratoren Sicherungs-Operatoren **Erforderlich:** Keine Änderung	**Standard:** Administratoren Sicherungs-Operatoren **Erforderlich:** Keine Änderung	**Standard:** (Nicht definiert) **Erforderlich:** Keine Änderung	**Standard:** Administratoren Sicherungs-Operatoren Server-Operatoren **Erforderlich:** Keine Änderung	Unterstützt die folgende TOE-Sicherheitsfunktionsanforderung: FMT_SMR.1, Sicherheitsrollen. Ein Missbrauch dieses Rechtes verletzt FDP_ACF.1(a), Zugriffssteuerung, da ein Benutzer die ACL-Einschränkungen

						umgehen kann. Implementiert die folgenden TOE-Sicherheitsfunktionen: Abs. 6.1.4.1, Rollen. Kann dazu verwendet werden, autorisierten Benutzern das Recht zu gewähren, Sicherungen durchzuführen. Weisen Sie dieses Recht keinen anderen Konten zu als den Standardkonten, um sicherzustellen, dass dieses Recht über die Mitgliedschaft in den Gruppen **Administratoren**, **Sicherungs-Operatoren** oder **Server-Operatoren** nur autorisierten Administratoren gewährt wird.
Sperren von Seiten im Speicher (SeLockMemoryPrivilege)	Ermöglicht es einem Prozess, Daten im physischen Arbeitsspeicher zu speichern, sodass das Auslagern von Daten in den virtuellen Speicher auf dem Datenträger durch das System verhindert wird.	**Standard**: Kein **Empfohlene Änderung**: Keine Änderung	**Standard**: Kein **Empfohlene Änderung**: Keine Änderung	**Standard**: (Nicht definiert) **Empfohlene Änderung**: Keine Änderung	**Standard**: Kein **Empfohlene Änderung**: Keine Änderung	

	Die Zuweisung dieses Rechtes kann zu einer erheblichen Beeinträchtigung der Systemleistung führen.					
Synchronisieren von Verzeichnisdienstdaten (SeSyncAgentPrivilege)	Ermöglicht es einem Dienst, Verzeichnissynchronisierungsdienste bereitzustellen. Dieses Recht ist nur auf Domänencontrollern von Bedeutung. Dieses Recht ist für einen Domänencontroller erforderlich, um die LDAP-Verzeichnissynchronisierungsdienste zu verwenden. Dieses Recht ermöglicht es dem Inhaber, unabhängig vom Schutz der Objekte und Eigenschaften alle Objekte und Eigenschaften im Verzeichnis zu lesen. Dieses Recht ist auf Domänencontrollern standardmäßig den Konten **Administratoren** und **LocalSystem** zugewiesen.	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** Kein **Empfohlene Änderung:** Keine Änderung	**Standard:** (Nicht definiert) **Empfohlene Änderung:** Keine Änderung	**Standard:** Administrator **Empfohlene Änderung:** Keine Änderung	
Übernehmen des Besitzes von Dateien und Objekten (SeTakeOwnershipPrivilege)	Ermöglicht es dem Benutzer, den Besitz von zu sichernden Objekten im System zu übernehmen, z. B. Active Directory-Objekte, Dateien und Ordner, Drucker,	**Standard:** Administratoren **Erforderlich:**	**Standard:** Administratoren **Erforderlich:**	**Standard:** (Nicht definiert) **Erforderliche**	**Standard:** Administratoren **Erforderlich:**	Unterstützt die folgende TOE-Sicherheitsfunktionsanforderung: FMT_SMR.1,

	Registrierungsschlüssel, Prozesse und Threads.	Keine Änderung	Keine Änderung	**Änderung:** Administratoren	Keine Änderung	Sicherheitsrollen. Ein Missbrauch dieses Rechtes verletzt FDP_ACF.1(a), Zugriffssteuerung, da ein Benutzer die ACL-Einschränkungen umgehen kann. Implementiert die folgenden TOE-Sicherheitsfunktionen: Abs. 6.1.4.1, Rollen. Kann verwendet werden, um autorisierten Benutzern die Möglichkeit zu gewähren, zu sichernde Objekte im System zu verwalten. **Änderungen:** Legen Sie die Domänenrichtlinie für dieses Recht auf **Administratoren** fest, damit eine vertrauenswürdige Verwaltung unterstützt wird.
Verändern der Firmwareumgebungsvariablen	Ermöglicht die Änderung von Systemumgebungsvariable	**Standard**:	**Standard**:	**Standard**:	**Standard**:	Unterstützt die folgende TOE-Sicherheitsfunktionsan

(SeSystemEnvironmentPrivilege)	n durch einen Prozess über eine API oder durch einen Benutzer über das Applet **Systemeigenschaften**.	Administratoren **Empfohlene Änderung**: Keine Änderung	Administratoren **Empfohlene Änderung**: Keine Änderung	(Nicht definiert) **Empfohlene Änderung**: Administratoren	Administratoren **Empfohlene Änderung**: Keine Änderung	forderung: FMT_SMR.1, Sicherheitsrollen. Implementiert die folgenden TOE-Sicherheitsfunktionen: Abs. 6.1.4.1, Rollen. Kann verwendet werden, um autorisierten Benutzern die Verwaltungsmöglichkeit zu gewähren, Systemumgebungsvariablen zu ändern. **Änderungen**: Legen Sie die Domänenrichtlinie für dieses Recht auf **Administratoren** fest, damit eine vertrauenswürdige Verwaltung unterstützt wird.
Verwalten von Überwachungs- und Sicherheitsprotokollen (SeSecurityPrivilege)	Ermöglicht es einem Benutzer, Überwachungsoptionen für den Objektzugriff einzelner Ressourcen anzugeben, wie z. B. Dateien, Active Directory-Objekte und	**Standard**: Administratoren **Erforderlich**: Keine Änderung	**Standard**: Administratoren **Erforderlich**: Keine Änderung	**Standard**: (Nicht definiert) **Erforderliche Änderung**: Administratoren	**Standard**: Administratoren **Erforderlich**: Keine Änderung	Unterstützt die folgende TOE-Sicherheitsfunktionsanforderung: FMT_SMR.1, Sicherheitsrollen,

	Registrierungsschlüssel. Die Überwachung des Objektzugriffs wird nur dann ausgeführt, wenn sie in der Überwachungsrichtlinie aktiviert wurde. Ein Benutzer mit diesem Recht kann außerdem das Sicherheitsprotokoll in der Ereignisanzeige anzeigen und löschen.					FAU_SAR.1.1, Überwachungsüberprüfung, FAU_SAR.2.1, Eingeschränkte Überwachungsüberprüfung; FAU_SAR.3, Wählbare Überwachungsüberprüfung; FAU_SEL.1, Selektive Überwachung, FAU_STG.1.1, FAU_STG.1.2, Garantien der Überwachungsverfügbarkeit FMT_MOF.1.1(a), Überwachungsverwaltung FMT_MOF.1.1(a), Verwaltung der Überwachungsliste FMT_MTD.1.1(b), Verwaltung von Überwachungsereignissen Implementiert die folgenden TOE-Sicherheitsfunktionen:

						Abs. 6.1.4.1, Rollen; und Abs. 6.1.1, Überwachungsfunktion. Kann verwendet werden, um autorisierten Benutzern die Verwaltungsmöglichkeit zu gewähren, Überwachungsdaten zu konfigurieren und zu verwalten. **Änderungen**: Legen Sie die Domänenrichtlinie für dieses Recht auf **Administratoren** fest, damit eine vertrauenswürdige Verwaltung unterstützt wird.
Wiederherstellen von Dateien und Verzeichnissen (SeRestorePrivilege)	Ermöglicht es einem Benutzer, beim Wiederherstellen gesicherter Dateien und Verzeichnisse die Datei- und Verzeichnisberechtigungen zu umgehen und einen gültigen Sicherheitsprinzipal als Besitzers eines Objekts festzulegen.	**Standard**: Administratoren Sicherungs-Operatoren **Erforderlich**: Keine Änderung	**Standard**: Administratoren Sicherungs-Operatoren **Erforderlich**: Keine Änderung	**Standard**: (Nicht definiert) **Erforderlich**: Keine Änderung	**Standard**: Administratoren Sicherungs-Operatoren Server-Operatoren **Erforderlich**: Keine Änderung	Unterstützt die folgende TOE-Sicherheitsfunktionsanforderung: FMT_SMR.1, Sicherheitsrollen. Ein Missbrauch dieses Rechtes verletzt FDP_ACF.1(a), Zugriffssteuerung, da ein Benutzer die ACL-Einschränkungen

						umgehen kann. Implementiert die folgenden TOE-Sicherheitsfunktionen: Abs. 6.1.4.1, Rollen. Kann dazu verwendet werden, autorisierten Benutzern das Recht zu gewähren, Sicherungen wiederherzustellen. Weisen Sie dieses Recht keinen anderen Konten zu als den Standardkonten, um sicherzustellen, dass dieses Recht über die Mitgliedschaft in den Gruppen **Administratoren**, **Sicherungs-Operatoren** und **Server-Operatoren** nur autorisierten Administratoren gewährt wird.