Anhang D – Benutzer- und Gruppenkonten

(Engl. Originaltitel: Appendix D - User and Group Accounts)

In Windows 2000 integrierte Benutzer und Gruppen	Beschreibung	Eigenständiges Professional-System	Eigenständiges Server-System	Domänen-controller	Standard-mitglieder	Anwendbarkeit auf Sicherheitszielanforderungen und/oder Gründe für Änderungen
Lokale Benutzerkonten	**Standardmäßige lokale Benutzerkonten.**					
Administrator	Integriertes Konto für die Verwaltung des Computers bzw. der Domäne	✓	✓	✓		Die Verwendung dieses Kontos durch mehr als einen autorisierten Administrator verletzt FAU_GEN.2, Benutzeridentitätszuordnung, da jedes überwachbare Ereignis der Identität des Benutzers zugeordnet werden muss, der das Ereignis verursacht hat. **Anforderung**: Weisen Sie autorisierten Administratoren Rollen zu, indem Sie ihre Benutzerkonten in für den jeweiligen Verantwortungsbereich geeigneten administrativen Gruppen platzieren. Dadurch wird sichergestellt, dass alle administrativen Vorgänge in Überwachungsprotokollen den jeweiligen Benutzerkonten zugeordnet werden können. Benennen Sie das Administratorkonto um, und sichern Sie das Kennwort zur ausschließlichen Verwendung in Notfällen.

Gast	Integriertes Konto für Gastzugriff auf den Computer bzw. die Domäne	✓	✓	✓		Ein Missbrauch dieses Kontos kann FAU_GEN.2, Benutzeridentitätszuordnung, FIA_UAU.2, Authentifizierung, und FIA_UID.2, Benutzeridentifizierung vor jedem Vorgang, verletzen. Dieses Konto ist auf allen Systemen standardmäßig deaktiviert. **Anforderung**: Dieses Konto muss deaktiviert bleiben.
TsInternetUser	Benutzerkonto, das von den Terminaldiensten verwendet wird. Dieses Konto wird für die Terminaldienste - Internet Connector-Lizenz verwendet. Wenn die Internet Connector-Lizenzierung aktiviert ist, akzeptiert ein Windows 2000-basierter Server 200 anonyme Verbindungen. Auf Terminaldienstclients wird kein Anmeldedialogfeld angezeigt, sondern sie werden automatisch		✓	✓		Die Verwendung dieses Kontos durch mehr als einen Benutzer verletzt FAU_GEN.2, Benutzeridentitätszuordnung. **Anforderung**: Die Terminaldienste sind nicht Gegenstand des TOE. Konten, die einen anonymen Zugriff unterstützen, dürfen nicht zugelassen werden. Deaktivieren Sie daher dieses Konto.

	mit dem Konto **TsInternetUser** angemeldet.					

krbtgt	Dienstkonto des Schlüsselverteilungscenters. Die Kerberos-Authentifizierung von Windows 2000 wird durch die Verwendung von Tickets erreicht, die mit einem symmetrischen Schlüssel verschlüsselt sind, der aus dem Kennwort des Servers oder Dienstes abgeleitet wird, auf den ein Zugriff angefordert wird. Um ein solches Sitzungsticket anzufordern, muss dem Kerberos-Dienst ein spezielles Ticket, das so genannte Ticket Granting Ticket (TGT), übergeben werden. Das TGT wird mit einem Schlüssel verschlüsselt, der vom Kennwort des Kontos **krbtgt** abgeleitet wird, das nur			✓		Die Verwendung dieses Kontos durch mehr als einen Benutzer verletzt FAU_GEN.2, Benutzeridentitätszuordnung. Dieses Konto ist auf Domänencontrollern standardmäßig deaktiviert. **Anforderung**: Im Gegensatz zu anderen Konten kann das Konto **krbtgt** nicht für die Anmeldung bei einer Domäne verwendet und de facto nicht deaktiviert werden.

	dem Kerberos-Dienst bekannt ist.					

Globale Gruppen	**Wenn eine Domäne erstellt wird, erstellt Windows 2000 die folgenden integrierten globalen Gruppen im Active Directory-Speicher, um häufige Typen von Benutzerkonten für die Verwendung in der gesamten Domäne zu gruppieren.**					**Globale Gruppen bieten die Möglichkeit, Benutzer zu autorisierten Administrator- und Benutzerrollen mit eindeutigen Zugriffsbeschränkungen auf Domänenebene zuzuweisen, die auf der globalen Gruppe basieren, der der Benutzer zugewiesen wurde. Globale Gruppen unterstützen die TOE-Sicherheitsfunktionsanforderung FMT_SMR.1, Sicherheitsrollen.**
Zertifikatherausgeber	Unternehmenszertifizierung und Erneuerungs-Agenten. Umfasst alle Computer, auf denen eine Unternehmenszertifizierungsstelle ausgeführt wird. Zertifikatherausgeber sind berechtigt, Zertifikate für Benutzerobjekte in Active Directory herauszugeben.			✓	Kein	Windows 2000 Certificate Server ist nicht Bestandteil der ausgewerteten Konfiguration.
DnsUpdateProxy	DNS-Clients, die dynamische Aktualisierungen für andere			✓	Kein	Das TOE unterstützt vollqualifizierte Domänennamen (Fully Qualified Domain Name oder FQDN) und erfordert keine

	Clients durchführen dürfen (wie etwa DHCP-Server).					Mitgliedschaft in dieser Gruppe. **Anforderung**: Fügen Sie dieser Gruppe keine Konten hinzu.

Domänen-Admins	Diese Gruppe ist nur auf Windows 2000-Servern verfügbar, die als Domänencontroller fungieren. Den Mitgliedern werden administrative Rechte für die gesamte Domäne gewährt. Diese Gruppe enthält standardmäßig das lokale Administratorkonto des Domänencontrollers als Mitglied.			✓	Administrator	Unterstützt die Zuweisung einer Administratorrolle mit Kontrollbefugnis in einer bestimmten Domäne. **Anforderung:** Fügen Sie dieser Gruppe nur Administratorkonten (keine Benutzer) hinzu.*
Domänencomputer	Alle Server und Arbeitsstationen der Domäne außer Domänencontrollern.			✓	Kein	Unterstützt die Zuweisung von Benutzerrollen, die den Zugriff auf domänencomputerspezifische Ressourcen unterstützen.
Domänencontroller	Gruppenkonto für alle Domänencontroller in der Domäne.			✓	Domänencontrollername	Unterstützt die Zuweisung von Benutzerrollen, die den Zugriff auf domänencontrollerspezifische Ressourcen unterstützen.
Domänen-Gäste	Diese Gruppe ist nur auf Windows 2000-Servern verfügbar, die als Domänencontroller fungieren. Mitgliedern dieser Gruppe			✓	Gast	Gastkonten/anonyme Konten können FAU_GEN.2, Benutzeridentitätszuordnung, FIA_UAU.2, Authentifizierung, und FIA_UID.2, Benutzeridentifizierung vor jedem Vorgang, verletzen. **Anforderung**:

	ist der Zugriff auf das System lediglich über das Netzwerk gestattet. Die Mitglieder verfügen standardmäßig über sehr beschränkte Rechte. Zu Beginn ist nur das Benutzerkonto **Gast** der Domäne enthalten.					Verwenden Sie diese Gruppe nicht. Entfernen Sie alle Konten einschließlich **Gast** aus dieser Gruppe.

Domänen-Benutzer	Diese Gruppe ist nur auf Windows 2000-Servern verfügbar, die als Domänencontroller fungieren. In einer Domänenumgebung werden das Administratorkonto und alle neuen Benutzerkonten automatisch als Mitglied in diese Gruppe aufgenommen. Diese Gruppe ist außerdem Mitglied der lokalen Benutzergruppe für die Domäne und für jeden Windows-Computer in der Domäne.			✓	Administrator Gast krbtgt TsInternetUser (Standardmäßig werden alle neuen Benutzer hinzugefügt.)	Unterstützt die Zuweisung von Benutzerrollen, die den Zugriff auf Domänenressourcen unterstützen. Gastkonten/anonyme Konten können FAU_GEN.2, Benutzeridentitätszuordnung, FIA_UAU.2, Authentifizierung, und FIA_UID.2, Benutzeridentifizierung vor jedem Vorgang, verletzen. **Anforderung**: Entfernen Sie die Konten **Gast** und **TsInternetUser**.
Organisations-Admins	Ermöglicht die administrative Kontrolle über das gesamte Netzwerk. Das Administratorkonto des Domänencontrollers ist standardmäßig Mitglied. Die Gruppe ist berechtigt, gesamtstrukturweite Änderungen			✓	Administrator (Domänencontroller)	Unterstützt die Zuweisung einer Administratorrolle mit Kontrollbefugnis über das gesamte Netzwerk.

	in Active Directory vorzunehmen, z. B. untergeordnete Domänen hinzuzufügen.					

Richtlinien-Ersteller-Besitzer	Mitglieder dieser Gruppe können Gruppenrichtlinien für die Domäne ändern. Die Gruppe mit der Berechtigung, neue Gruppenrichtlinienobjekte in Active Directory zu erstellen.			✓	Administrator	Unterstützt die Zuweisung einer Administratorrolle für die Verwaltung der Gruppenrichtlinien auf Domänenebene. **Anforderung**: Fügen Sie dieser Gruppe nur Administratorkonten hinzu.*
Schema-Admins	Designierte Administratoren des Active Directory-Schemas. Diese Gruppe ist berechtigt, Schemaänderungen in Active Directory vorzunehmen.			✓	Administrator	Unterstützt die Zuweisung einer Administratorrolle für die Verwaltung des Active Directory-Schemas. **Anforderung**: Fügen Sie dieser Gruppe nur Administratorkonten hinzu.*
Domänenlokale Gruppen	**domänenlokale Gruppen stellen Benutzern die Rechte und Berechtigungen für die Durchführung von Aufgaben insbesondere auf dem Domänencontroller und im Active Directory-Speicher zur Verfügung.**					**domänenlokale Gruppen bieten die Möglichkeit, Benutzer zu autorisierten Administrator- und Benutzerrollen mit eindeutigen Zugriffsbeschränkungen für den Domänencontroller zuzuweisen, die auf der lokalen Domänengruppe basieren, der der Benutzer zugewiesen wurde. Lokale Domänengruppen unterstützen die TOE-Sicherheitsfunktionsanforderung FMT_SMR.1, Sicherheitsrollen.**
Administratoren	Die Mitglieder können alle administrative			✓	Administrator	Unterstützt die Zuweisung einer Administratorrolle mit vollständigen administrativen

	n Aufgaben auf allen Domänencontrollern und durchführen.				Domänen-Admins Organisations-Admins	Zugriffsrechten auf alle Domänencontroller in einer Domäne. **Anforderung**: Fügen Sie dieser Gruppe nur Administratorkonten hinzu.*
Benutzer	Diese Gruppe gewährt einem Benutzer die erforderlichen Rechte, um als Endbenutzer mit dem Computer zu arbeiten, z. B. Anwendungen auszuführen und Dateien zu verwalten. In Windows 2000 werden standardmäßig alle neuen Benutzerkonten zu der Gruppe **Benutzer** hinzugefügt.			✓	Authentifizierte Benutzer Domänen-Benutzer INTERAKTIV (Standardmäßig werden alle neuen lokalen Benutzer hinzugefügt.)	Unterstützt die Zuweisung von Benutzerrollen, die den Zugriff auf Ressourcen des Domänencontrollers unterstützen. **Anforderung**: Fügen Sie dieser Gruppe keine Konten mit möglicherweise nicht authentifiziertem Zugriff (wie z. B. **Gast**) hinzu.
DnsAdmins	DNS-Administratorengruppe. Diese Gruppe verfügt über Vollzugriff auf einen DNS-Server und seine Zonen.			✓	Kein	Unterstützt die Zuweisung einer Administratorrolle, die für die Verwaltung von DNS verantwortlich ist. **Anforderung**: Fügen Sie dieser Gruppe nur Administratorkonten hinzu.*
Druck-	Eine			✓	Kein	Unterstützt die Zuweisung

Operatoren	vordefinierte Gruppe, die nur auf Domänencontrollern vorhanden ist. Die Mitglieder können Netzwerkdrucker auf Domänencontrollern einrichten und verwalten. Die Mitglieder dieser Gruppe erhalten die Rechte, Druckerfreigaben in der Domäne zu erstellen, zu ändern und zu löschen. Die Mitglieder können sich auch lokal an Systemen anmelden und sie herunterfahren.					einer Administratorrolle, die für die Verwaltung der Druckdienste in einer Domäne verantwortlich ist. **Empfehlung**: Hierbei handelt es sich um eine administrative Funktion. Fügen Sie daher nur autorisierte Administratoren zu dieser Gruppe hinzu.
Gäste	Die Gruppe **Gäste** bietet begrenzten Zugriff auf die Ressourcen des Systems. Die Mitglieder können keine dauerhaften Änderungen an ihrer Desktopumgebung vornehmen. Einige Dienste fügen bei der Installation automatisch			✓	Gast (lokal) Domänen-Gäste TsInternetUser	Gastkonten/anonyme Konten können FAU_GEN.2, Benutzeridentitätszuordnung, FIA_UAU.2, Authentifizierung, und FIA_UID.2, Benutzeridentifizierung vor jedem Vorgang, verletzen. **Anforderung**: Verwenden Sie diese Gruppe nicht. Entfernen Sie alle Konten einschließlich **Gast** aus dieser Gruppe.

	Benutzer zu dieser Gruppe hinzu. IIS fügt beispielsweise die anonymen Benutzerkonten zur vordefinierten Gruppe **Gäste** hinzu.					
Konten-Operatoren	Diese Gruppe ist nur auf Windows 2000-Servern verfügbar, die als Domänencontroller fungieren. Sie ermöglicht den Mitgliedern die Verwaltung von Benutzer- und Gruppenkonten für Systeme und Domänen. Konten-Operatoren verfügen standardmäßig über das Recht, in allen Containern und Organisationseinheiten von Active Directory außer dem Container **Vordefiniert** und der Organisationseinheit **Domänencontroller** Konten für Benutzer,			✓	Kein	Unterstützt die Zuweisung einer Administratorrolle für die Verwaltung von Benutzerkonten in einer Domäne. **Anforderung:** Fügen Sie dieser Gruppe nur Administratorkonten hinzu.*

	Gruppen und Computer zu erstellen, zu ändern und zu löschen. Konten-Operatoren besitzen nicht das Recht, die Gruppen **Administratoren** und **Domänen-Admins** bzw. die Konten für Mitglieder dieser Gruppen zu ändern.					
Prä-Windows 2000 kompatibler Zugriff	Eine Gruppe, die beschränkten Lesezugriff auf Objekte im Active Directory hat und so die Kompatibilität zu Vorgängerversionen. ermöglicht.			✓	Kein	**Anforderung**: Die Abwärtskompatibilität mit Vorgängerversionen von Windows 2000-Systemen ist nicht Gegenstand des TOE. Fügen Sie daher keine Benutzer zu dieser Gruppe hinzu.
RAS- und IAS-Server	Server in dieser Gruppe können auf die RAS-Eigenschaften von Benutzern zugreifen.			✓	Kein	
Replikations-Operator	Dieses Konto wird für den Dateireplikationsdienst von Domänencontrollern verwendet. Die Mitglieder können die Dateireplikati			✓	Kein	Kann zur Unterstützung der Anforderungen in Abs. 6.1.5.3, TFS-Datenreplikationskonsistenz, verwendet werden. Unterstützt die Zuweisung einer Administratorrolle, die für die Verwaltung der Verzeichnisreplikationsdienste in einer Domäne

	onsdienste konfigurieren. Der Verzeichnisreplikationsdienst sorgt automatisch für das Kopieren von Dateien, z. B. Benutzeranmeldeskripts, zwischen Windows 2000-basierten Computern.					verantwortlich ist. **Anforderung**: Fügen Sie dieser Gruppe nur Administratorkonten hinzu.*
Server-Operatoren	Diese Gruppe ist nur auf Windows 2000-Servern verfügbar, die als Domänencontroller fungieren. Die Mitglieder dieser Gruppe können Serververwaltungsaufgaben durchführen, wie z. B. das Erstellen, Ändern und Löschen von freigegebenen Druckern, freigegebenen Verzeichnissen und Dateien. Sie können außerdem Dateien sichern und wiederherstellen, die Serverkonsole sperren und das System herunterfahren			✓		Unterstützt die Zuweisung einer Administratorrolle, die für die Serververwaltung verantwortlich ist. **Anforderung**: Fügen Sie dieser Gruppe nur Administratorkonten hinzu.*

	. Sie können keine Systemrichtlinien ändern oder Dienste starten oder beenden.					
Sicherungs-Operatoren	Die Mitglieder können mit der Windows-Sicherung Dateien auf allen Domänencontrollern sichern und wiederherstellen, unabhängig von den Rechten zum Schutz dieser Dateien. Sicherungs-Operatoren können sich auch am Computer anmelden und ihn herunterfahren.			✓	Kein	Ein Missbrauch dieses Kontos kann FDP_ACF.1(a), Zugriffssteuerung, verletzen. Ein Mitglied der Gruppe **Sicherungs-Operator** kann Dateien und Verzeichnisse extrahieren, auf die der Benutzer normalerweise nicht zugreifen kann. Die Mitgliedschaft in dieser Gruppe gestattet es Benutzern, jede Datei für Sicherungszwecke zu öffnen. Nachdem die Datei für einen Lesezugriff geöffnet wurde, kann sie vom Sicherungs-Operator jedoch an einen beliebigen Speicherort umgeleitet werden. Benutzer dürfen standardmäßig die Dateien sichern und wiederherstellen, für die sie die entsprechenden Datei- und Verzeichnisrechte besitzen, ohne dass die Mitgliedschaft in der Gruppe **Sicherungs-Operatoren** erforderlich ist. Das Administratorkonto verfügt bereits über vollständige Sicherungsrechte. **Anforderung**: Fügen Sie dieser Gruppe nur Administratorkonten hinzu.*
Lokale Gruppen	**Alle eigenständige**					**Lokale Gruppen bieten die Möglichkeit, Benutzer zu**

	n Windows 2000-Server, Mitgliedsserver und Professional-Arbeitsstationen verfügen über vordefinierte lokale Gruppen. Diese vordefinierten lokalen Gruppen ermöglichen den Mitgliedern das Ausführen von Aufgaben auf dem jeweiligen Computer, zu dem die Gruppe gehört.					**autorisierten Administrator- und Benutzerrollen mit eindeutigen lokalen Zugriffsbeschränkungen zuzuweisen, die auf der lokalen Gruppe basieren, der der Benutzer zugewiesen wurde. Lokale Gruppen unterstützen die TOE-Sicherheitsfunktionsanforderung FMT_SMR.1, Sicherheitsrollen.**
Administratoren	Mitglieder der Gruppe **Administratoren** verfügen über Vollzugriff auf den gesamten Computer. Wenn ein Mitgliedsserver oder ein Computer unter Windows 2000 einer Domäne beitritt, wird die Gruppe **Domänen-Admins** zu	✓	✓		**Eigenständig**: Administrator **Domänenmitglieder**: Administrator Domänen-Admins	Unterstützt die Zuweisung einer Administratorrolle mit vollständigen administrativen Zugriffsrechten auf alle lokalen Ressourcen eines Computers. **Anforderung**: Fügen Sie dieser Gruppe nur Administratorkonten hinzu.*

	der lokalen Gruppe **Administratoren** hinzugefügt.					
Benutzer	Diese Gruppe gewährt einem Benutzer die erforderlichen Rechte, um als Endbenutzer mit dem Computer zu arbeiten, z. B. Anwendungen auszuführen und Dateien zu verwalten. In Windows 2000 werden standardmäßig alle neuen Benutzerkonten zu der Gruppe **Benutzer** hinzugefügt. Wenn ein Mitgliedsserver oder ein Computer unter Windows 2000 einer Domäne beitritt, werden die globale Gruppe **Domänen-Benutzer**, die spezielle Gruppe **Authentifizierte Benutzer** und die spezielle Gruppe **INTERAKTI**	✓	✓		**Eigenständig:** Authentifizierte Benutzer INTERAKTIV (Standardmäßig werden alle neuen lokalen Benutzer hinzugefügt.) **Domänenmitglieder:** Authentifizierte Benutzer Domänen-Benutzer INTERAKT	Unterstützt die Zuweisung von Benutzerrollen, die den Zugriff auf lokale Ressourcen des Computers unterstützen. **Anforderung**: Fügen Sie dieser Gruppe keine Konten mit möglicherweise nicht authentifiziertem Zugriff (wie z. B. **Gast**) hinzu.

	V zu der lokalen Gruppe **Benutzer** hinzugefügt.				IV (Standardmäßig werden alle neuen lokalen Benutzer hinzugefügt.)	
Gäste	Die Gruppe **Gäste** bietet begrenzten Zugriff auf die Ressourcen des Systems. Die Mitglieder können keine dauerhaften Änderungen ihrer Desktopumgebung vornehmen. Das Benutzerkonto **Gast** des Computers ist standardmäßig Mitglied. Dieses Konto ist standardmäßig deaktiviert.	✓	✓		**Eigenständiges Professional-System:** Gast **Eigenständiger Server:** Gast TsInternetUser **Domänenmitglieder:** Weitere Domänen-Gäste	Gastkonten/anonyme Konten können FAU_GEN.2, Benutzeridentitätszuordnung, FIA_UAU.2, Authentifizierung, und FIA_UID.2, Benutzeridentifizierung vor jedem Vorgang, verletzen. **Anforderung**: Verwenden Sie diese Gruppe nicht. Entfernen Sie alle Konten einschließlich **Gast** aus dieser Gruppe.
Hauptbenutzer	Die Mitgliedschaft ermöglicht es	✓	✓		Kein	Unterstützt die Zuweisung von Benutzerrollen mit höheren Zugriffsrechten auf

	Benutzern, lokale Benutzerkonten im Computer zu erstellen und zu ändern sowie Ressourcen freizugeben, ohne dass der Benutzer Vollzugriff auf den Computer erhält.					einem bestimmten Computer. Diese Gruppe gewährt Rechte auf Administratorebene, wie z. B. die Verwaltung lokaler Benutzerkonten und lokaler Ressourcen. Die Mitgliedschaft von Benutzern in dieser Gruppe, die keine autorisierten Administratoren sind, verletzt FMT_MTD.1(c), Verwaltung von Benutzerattributen, FMT_MTD.1(d), Verwaltung von Authentifizierungsdaten (für benutzererstellte Konten), FMT_MTD.1(e), Verwaltung der Kontosperrdauer (für benutzererstellte Konten), Verwaltung der minimalen Kennwortlänge (für benutzererstellte Konten), und FMT_SMR.1, Sicherheitsrollen, in dem Maße wie dem Gewähren von Rechten für Benutzer, die normalerweise zu einer autorisierten Administratorrolle gehören. **Anforderung**: Fügen Sie dieser Gruppe nur Administratorkonten hinzu.*
Replikations-Operator	Die Mitglieder können die Dateireplikationsdienste konfigurieren. Der Verzeichnisreplikationsdienst sorgt automatisch für das Kopieren von Dateien, z. B. Benutzeranmeldeskripts, zwischen	✓	✓		Kein	Kann zur Unterstützung der Anforderungen in Abs. 6.1.5.3, TFS-Datenreplikationskonsistenz, verwendet werden. Unterstützt die Zuweisung einer Administratorrolle, die für die Verwaltung der Verzeichnisreplikationsdienste in einem Computer verantwortlich ist. **Anforderung**: Fügen Sie dieser Gruppe nur Administratorkonten hinzu.*

	Windows 2000-basierten Computern.					
Sicherungs-Operatoren	Die Mitglieder können den Computer mit der Windows-Sicherung unabhängig von der Dateisystemsicherheit sichern und wiederherstellen.	✓	✓		Kein	Ein Missbrauch dieses Kontos kann FDP_ACF.1(a), Zugriffskontrolle, verletzen. Ein Mitglied der Gruppe **Sicherungs-Operatoren** kann Dateien und Verzeichnisse extrahieren, auf die der Benutzer normalerweise nicht zugreifen kann. Die Mitgliedschaft in dieser Gruppe gestattet es Benutzern, jede Datei für Sicherungszwecke zu öffnen. Nachdem die Datei für einen Lesezugriff geöffnet wurde, kann sie vom Sicherungs-Operator jedoch an eine beliebige Position umgeleitet werden. Benutzer dürfen standardmäßig die Dateien sichern und wiederherstellen, für die sie die entsprechenden Datei- und Verzeichnisrechte besitzen, ohne dass die Mitgliedschaft in der Gruppe **Sicherungs-Operatoren** erforderlich ist. Das Administratorkonto verfügt bereits über vollständige Sicherungsrechte. **Anforderung**: Fügen Sie dieser Gruppe nur Administratorkonten hinzu.*
Systemgruppen	**Systemgruppen weisen keine speziellen Zugehörigkei**					

	ten auf, die verändert werden können. Jede Systemgruppe dient der Darstellung einer speziellen Klasse von Benutzern bzw. der Darstellung des Betriebssystems. Diese Gruppen werden von Windows 2000-Systemen automatisch erstellt, auf der Benutzeroberfläche für die Gruppenverwaltung jedoch nicht angezeigt.					
Anonymous-Anmeldung	Enthält alle Benutzerkonten, die von Windows 2000 nicht authentifiziert wurden.	✓	✓	✓	Alle nicht authentifizierten Benutzer.	Ein Missbrauch dieses Kontos kann FAU_GEN.2, Benutzeridentitätszuordnung, FIA_UAU.2, Authentifizierung, und FIA_UID.2, Benutzeridentifizierung vor jedem Vorgang, verletzen. **Anforderung:** Gewähren Sie diesem Konto keine Rechte für Ressourcen oder Benutzerrechte.
Authentifizierte Benutzer	Enthält alle Benutzer mit einem gültigen Konto im Computer	✓	✓	✓	Alle authentifizierten Benutzer.	Unterstützt FAU_GEN.2, Benutzeridentitätszuordnung, FIA_UAU.2, Authentifizierung, und FIA_UID.2, Benutzeridentifizierung.

	bzw. in Active Directory-Diensten.					**Empfehlung:** Verwenden Sie die Gruppe **Authentifizierte Benutzer** anstelle der Gruppe **Jeder**, um einen anonymen Zugriff auf eine Ressource zu verhindern.
BATCH	Eine Gruppe mit allen Benutzern, die anhand einer Batchwartesch lange anmeldet wurden.	✓	✓	✓		
DIALUP	Enthält alle Benutzer, die zurzeit über eine DFÜ-Verbindung auf das Netzwerk zugreifen.	✓	✓	✓	Alle DFÜ-Benutz er.	**Anforderung:** Die Unterstützung von DFÜ-Diensten ist nicht Gegenstand des TOE. Gewähren Sie diesem Konto daher keine Rechte für Ressourcen oder Benutzerrechte.
DIENST	Eine Gruppe, die alle Sicherheitspri ncipals enthält, die als Dienst angemeldet sind.	✓	✓	✓		
DOMÄNENCO NTROLLER DER ORGANISATI ON	Eine Gruppe mit allen Domänencontr ollern in einer Gesamtstruktu r, die einen Active Directory-Dienst verwendet.			✓		
EINGESCHRÄ NKTER ZUGRIFF	Diese SID wird in Windows 200 0 nicht verwendet.			✓		
ERSTELLER-	Enthält das	✓	✓	✓	Mitgli	Unterstützt FDP_ACF.1(a),

BESITZER	Benutzerkonto eines Benutzers, der eine Ressource erstellt oder den Besitz einer Ressource übernommen hat. Wenn ein Mitglied der Gruppe **Administratoren** eine Ressource erstellt, ist die Gruppe **Administratoren** Besitzer der Ressource. Diese Gruppe wird für jede freigebbare Ressource in Windows 2000 Server oder Professional erstellt. Ein Platzhalter in einem erbbaren Zugriffssteuerungseintrag (ACE oder Access Control Entry). Wenn der ACE geerbt wird, ersetzt das System diese SID durch die SID des Objektstellers.				eder dieser Gruppe sind Benutzer, die Ressourcen erstellen oder den Besitz von Ressourcen übernehmen.	Wahlweise Zugriffsliste, durch die Zuweisung von Objektbesitzerattributen.
ERSTELLERGRUPPE	Ein Platzhalter in einem erbbaren Zugriffssteuer	✓	✓	✓		

	ungseintrag (ACE oder Access Control Entry). Wenn der ACE geerbt wird, ersetzt das System diese SID durch die SID der primären Gruppe des Objektstellers.					
INTERAKTIV	Enthält das Benutzerkonto des Benutzers, der lokal am Computer angemeldet ist. Die Mitglieder der Gruppe **INTERAKTIV** erhalten Zugriff auf die Ressourcen des Computers, an dem sie physisch arbeiten.	✓	✓	✓	Diese Gruppe enthält alle Benutzer, die sich lokal bei Windows 2000 Server oder Professional anmelden. Benutzer, die über ein Netzwerk verbunden sind, gehören nicht zu dieser Gruppe.	

Jeder	Enthält alle Benutzer, die auf den Computer zugreifen. Windows 2000 authentifiziert einen Benutzer ohne gültiges Benutzerkonto als Gast. Der Benutzer erhält automatisch alle Rechte und Berechtigungen, die der Gruppe **Jeder** zugewiesen sind. Eine Gruppe, die alle Benutzer enthält, auch anonyme Benutzer und Gäste.	✓	✓	✓	Die Mitglieder dieser Gruppe umfassen alle Benutzer, die lokal, über das Netzwerk oder über RAS auf Windows 2000 Server oder Professional zugreifen. Dazu gehören authentifizierte und nicht authentifizierte Benutzer. De facto ist jeder Benutzer, der auf das System zugreif	Ein Missbrauch dieses Kontos kann FAU_GEN.2, Benutzeridentitätszuordnung, FIA_UAU.2, Authentifizierung, und FIA_UID.2, Benutzeridentifizierung vor jedem Vorgang, verletzen. **Anforderung:** Gewähren Sie diesem Konto keine Rechte für Ressourcen oder Benutzerrechte. Verwenden Sie bei Bedarf **Authentifizierte Benutzer** bzw. spezielle Benutzerkonten und Gruppen.

					t, Mitglied der Gruppe **Jeder**.	
NETZWERK	Enthält alle Benutzer mit einer aktiven Verbindung von einem anderen Computer im Netzwerk mit einer freigegebenen Ressource des Computers.	✓	✓	✓	Diese Gruppe enthält alle Benutzer, die über ein Netzwerk mit Ressourcen verbunden sind, aber keine Benutzer, die interaktiv verbunden sind.	
PROXY	Diese SID wird in Windows 2000 nicht verwendet.			✓		
SELBST	Ein Platzhalter in einem erbbaren ACE eines Kontoobjekts oder Gruppenobjekts in Active Directory. Wenn der ACE geerbt wird, ersetzt			✓		

	das System diese SID durch die SID des Sicherheitsprinzipals, der das Konto enthält.					
SYSTEM	Ein Konto, das vom Betriebssystem für die Ausführung von Diensten, Dienstprogrammen und Gerätetreibern verwendet wird. Dieses Konto verfügt über unbegrenzte Berechtigungen und Zugriff auf Ressourcen, der selbst Administratoren verweigert wird, z. B. auf die Sicherheitskontenverwaltung der Registrierung.	✓	✓	✓		Dieses Konto wird von Windows 2000 für die Ausführung von Sicherheitsdiensten wie TSF-Schutzfunktionen verwendet, die außerhalb des Zugriffs autorisierter Administratoren liegen.
TERMINALSERVERBENUTZER		✓	✓	✓		**Anforderung**: Die Unterstützung der Terminaldienste ist nicht Gegenstand des TOE. Gewähren Sie diesem Konto daher keine Rechte für Ressourcen oder Benutzerrechte.

* Es ist nicht erforderlich, die entsprechende Gruppe aus den Zugriffssteuerungslisten für den (Discretionary Access Control List oder DACL) gesicherter Objekte zu entfernen, solange diese Anforderung erfüllt wird.