Anleitung zur IDM Gruppenverwaltung

Version 1.3.1
Datum: 12.10.2022

TECHNISCHE UNIVERSITÄT DARMSTADT

HRZ Hochschulrechenzentrum

Technische Universität Darmstadt
Hochschulrechenzentrum
Alexanderstraße 2
64283 Darmstadt

http://www.hrz.tu-darmstadt.de
service@hrz.tu-darmstadt.de

Inhaltsverzeichnis

Änderungshistorie

Für eine bessere Transparenz unserer Serviceangebote, werden Änderungen zur letzten veröffentlichten Version hier zusammengefasst.

Datum	Version	Bearbeiter_in	Änderung
19.08.2022	1.0	WB	Initialversion
14.09.2022	1.1	ClB	Neue Grafiken
05.10.2022	1.2	ClB	Vervollständigung
07.10.2022	1.3.0	ClB	Beispiele eingefügt
12.10.2022	1.3.1	WB	Review und kleine Korrekturen, Typos etc.

1. Kurzbeschreibung der IDM Gruppenverwaltung

Die Gruppenverwaltung im IDM-Portal bietet den Nutzer*innen innerhalb und außerhalb des HRZ die Möglichkeit TU-IDs in Gruppen zu organisieren und diese Gruppen an Services anzubinden. Diese Gruppen werden über das IDM-Portal verwaltet und im LDAP und AD als auch über den SSO dem Service zur Verfügung gestellt.

2. Zielgruppe für die IDM Gruppenverwaltung

Zielgruppen für die Verwendung der IDM Gruppenverwaltung sind die HRZ Kunden. Die Kunden sind im ERP System des HRZs angelegt und haben eine eindeutige Kundennummer. Die Kunden brauchen eine Möglichkeit alle Arten von Zugriffsberechtigungen in ihren Bereichen automatisiert zu verwalten. Dazu können sie die IDM Gruppenverwaltung benutzen, die ihnen ermöglicht Gruppierungen für ihre Bereiche zu schaffen und dann die Berechtigungen für ihre Services den Gruppen zuweisen.

Kunden sind u.a.

- Einrichtungen der TU (Fachbereiche, zentrale Einrichtungen)
- Zentralverwaltung

3. Rahmenbedingungen (Voraussetzungen)

Nur Angehörige der TU Darmstadt mit einer TU-ID, die zum Kundenstamm des HRZs gehören, können die IDM Gruppenverwaltung nutzen.
Pro Kunde müssen zwei Kundenbeauftragte benannt werden.
Auf Grund der Komplexität der Gruppenverwaltung gibt es eine Schulung für zukünftige Kundenbeauftragte. Die Schulung von zweimal 90 Minuten erklärt die Konzepte zunächst theoretisch und anschließend praktisch am Testsystem. Bevor jemand als Kundenbeauftragte*r definiert wird, ist es wichtig, dass diese Person an der Schulung teilgenommen hat.
Wenn Sie Interesse an der Nutzung der IDM-Gruppen und den nächsten Schulungsterminen haben, fragen Sie einfach via HRZ-Service an.

4. Funktionsweise

Die Kernaufgabe des IDMs ist die Authentifizierung einer Person und die Bereitstellung von, zur Identität dieser Person gehörigen, Eigenschaften (Attributen) an die angeschlossenen Services.
Die Berechtigungsvergabe für einzelne Anwender*innen für einzelne Dienste gehört nicht zu den Aufgaben eines IDM Systems. Diese Zuordnung von Rechten an Personen (Autorisierung) ist Aufgabe der Services. Um diese Aufgabe zu erledigen, kann sich der Service der vom IDM gelieferten Attribute

bedienen.
Da einige Services aber keine ausreichende Nutzungsschnittstelle zur Verwaltung ihrer Rechte haben, wird für diese Services der Service ”IDM Gruppenverwaltung” zur Verfügung gestellt. Das bedeutet, es werden weitere Attribute (in Form von Gruppenmitgliedschaften) geliefert, welche dann von den Services genutzt werden können, um Rechte daran zu knüpfen.
Das IDM System selbst hat keinen Einfluss darauf ob/wie die Services tatsächlich die Gruppen- oder andere Attribute für Berechtigungen nutzen. Daher ist die IDM Gruppenverwaltung nur eine Möglichkeit der Strukturierung für die Gruppen, aber diese Gruppen können nicht die vollständigen Rechte einer Person abbilden. Die jeweilige Rechtezuordnung erfolgt ausschließlich in den Services.

4.1. Welche Arten von Gruppen gibt es

4.1.1. Organisatorische Gruppen

Diese Gruppen werden automatisch vom IDM anhand der Identität der Person und deren organisatorischer Zugehörigkeit bereitgestellt. Die Datenquelle ist das SAP-HCM, d.h. die Daten werden vom IDM nur übernommen. Auf deren Richtigkeit und Änderung hat das IDM System keinen Einfluss.
Bei einem organisatorischen Wechsel der Person oder bei Verlassen der TU werden die organisatorischen Gruppen automatisch angepasst.
Für die Nutzer der IDM Gruppenverwaltung hat das den großen Vorteil, dass sie sich nicht um darum kümmern müssen.

4.1.2. Servicegruppen

Diese Gruppen werden von Servicebeauftragten eines Services erstellt gepflegt. Der Service kann ein HRZ Service oder der einer Kund*in sein. Die Servicegruppen dienen der Zuordnung von Rechten (oder Funktionen) und werden entfernt wenn der Service eingestellt wird. Es ist sehr wichtig, dass sowohl der Anzeigename als auch die Beschreibung der Servicegruppe aussagekräftig gewählt wird. Eine korrekte Benennung und anschließend konsistente Konfiguration des Services kann der Anwender*in ein gutes Verständnis ihrer Berechtigungen geben.
Eine geschickt gewählte generische Benennung dieser Gruppe und auch die Zuordnung kann bei organisatorischen Änderungen dazu führen die Servicegruppen beibehalten zu können und somit eine Konfigurationsänderung am Service zu verhindern. Daher wird empfohlen diese Gruppen mit Kundengruppen statt direkt mit TU-IDs zu befüllen. Das erleichtert auch die Aufteilung der Pflegeverantwortlichkeit.

Beispiele für Servicegruppennamen wären etwa:

- Schreibrechte auf Netzlaufwerk Sekretariat
- Empfänger Mailverteiler Leitung
- Urlaube in HR-System genehmigen

4.1.3. Kundengruppen

Diese Gruppen werden vom Kundenbeauftragten erstellt und von den Gruppenbeauftragten gepflegt. Die Struktur der Kundengruppen ist kundenspezifisch.
Häufig lassen sich Zugriffe auf verschiedene Systeme anhand von Rollen zuschneiden. Beispielsweise darf eine Sachbearbeiter*in der Personalabteilung sowohl Schreibrechte auf ein Dateiverzeichnis haben, als auch Vertragsdaten im HR-System ändern. Eine Sachbearbeiter*in in einer anderen Einrichtung darf aber vielleicht auch in das Verzeichnis schreiben, aber im HR-System nur Urlaube beantragen. Um nicht bei jeder personellen Änderung die einzelne Person in vielen Servicegruppen pflegen zu müssen werden diese über Gruppen zusammengefasst.
Zusätzlich kann die Pflege dieser Gruppen von der personell verantwortlichen Person erledigt werden

und so die Servicebeauftragten entlasten. Um die Pflege noch weiter zu erleichtern können solche Rollengruppen automatisch gepflegte organisationsweite Gruppen enthalten und nur um einzelne Mitarbeiter*innen (z.B. Kolleg*innen aus anderen Abteilungen oder Studierende) ergänzt werden.

Beispiele für Kundengruppennamen wären etwa:

- Leitung Hochschulrechenzentrum
- Sachbearbeiter:innen Personalwesen

4.2. Verantwortliche und beauftragte Personen für Gruppen

Das Administrieren, also das Erstellen und Zuordnen von IDM Gruppen können nur die im Folgenden beschriebenen Personengruppen übernehmen.
In IDM Gruppen eingeordnet werden, kann jeder TU Angehörige.

4.2.1. Kundenbeauftragte

Kundenbeauftragte sind für die Erstellung von Kundengruppen und Services zuständig und verantwortlich. Weiterhin benennen sie Servicebeauftragte und Gruppenbeauftragte. Sie sind immer TU mitarbeitende natürliche Personen aber niemals Gruppen. Mit Kunden sind hier Kunden des HRZs gemeint. Die Kundenbeauftragten des HRZs sind das ÍDM Team, die Kundenbeauftragten der zV ist die APB oder Experten aus dem HRZ.
Folgende Kunden werden von den Kundenbeauftragten administriert:

- Einrichtungen der TU (Fachbereiche, zentrale Einrichtungen)
- Zentralverwaltung

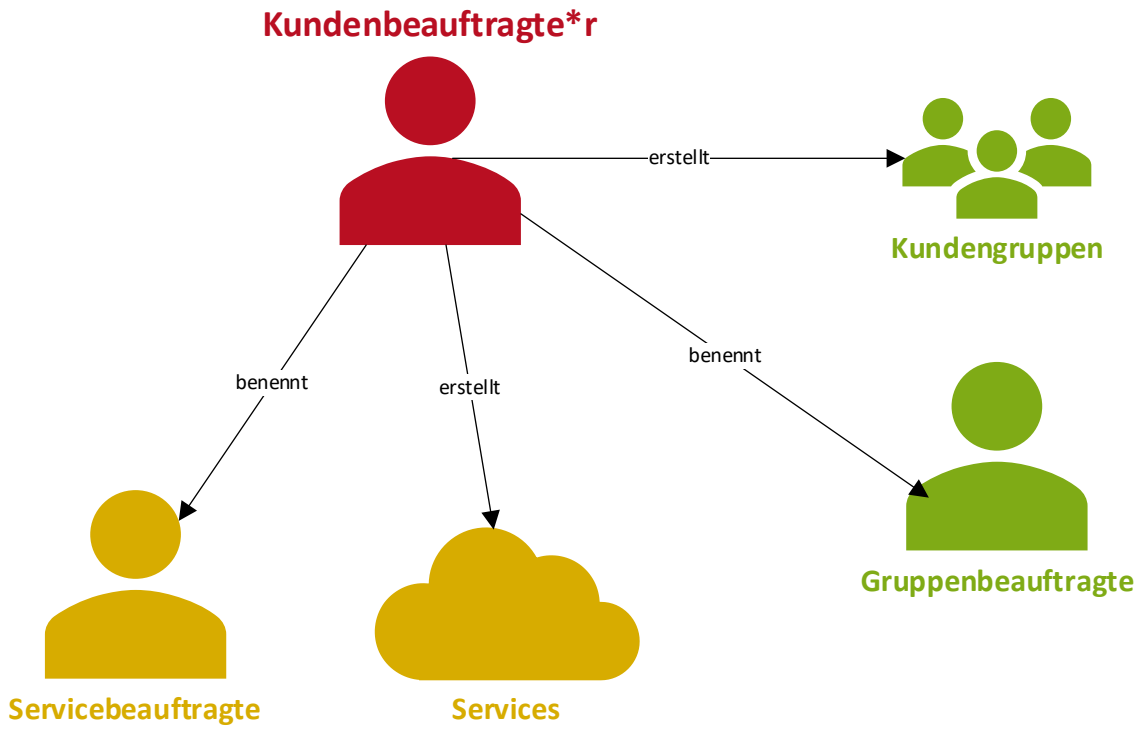

Diagramm1: Kundenbeauftragte

4.2.2. Servicebeauftragte

Die Servicebeauftragten erstellen die Servicegruppen. Der Service selbst wird (bzw. wurde vorher) vom Kundenbeauftragten erstellt.

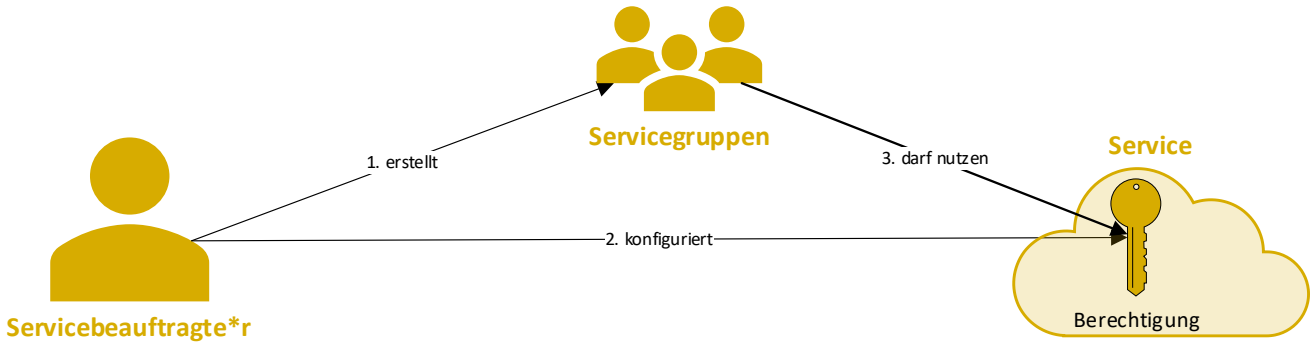

Diagramm2: Servicebeauftragte

Die Administration von den Servicegruppen wird von Servicebeauftragten übernommen. Der Servicebeauftragte kann folgende Zuordnungen treffen:

- Einzelne Personen anhand ihrer TU-ID
- TechIDs
- Servicegruppen (Schachtelungstiefe von 3 darf nicht überschritten werden)
- Kundengruppen (Schachtelungstiefe von 5 darf nicht überschritten werden)

können einer Servicegruppe zugeordnet werden.

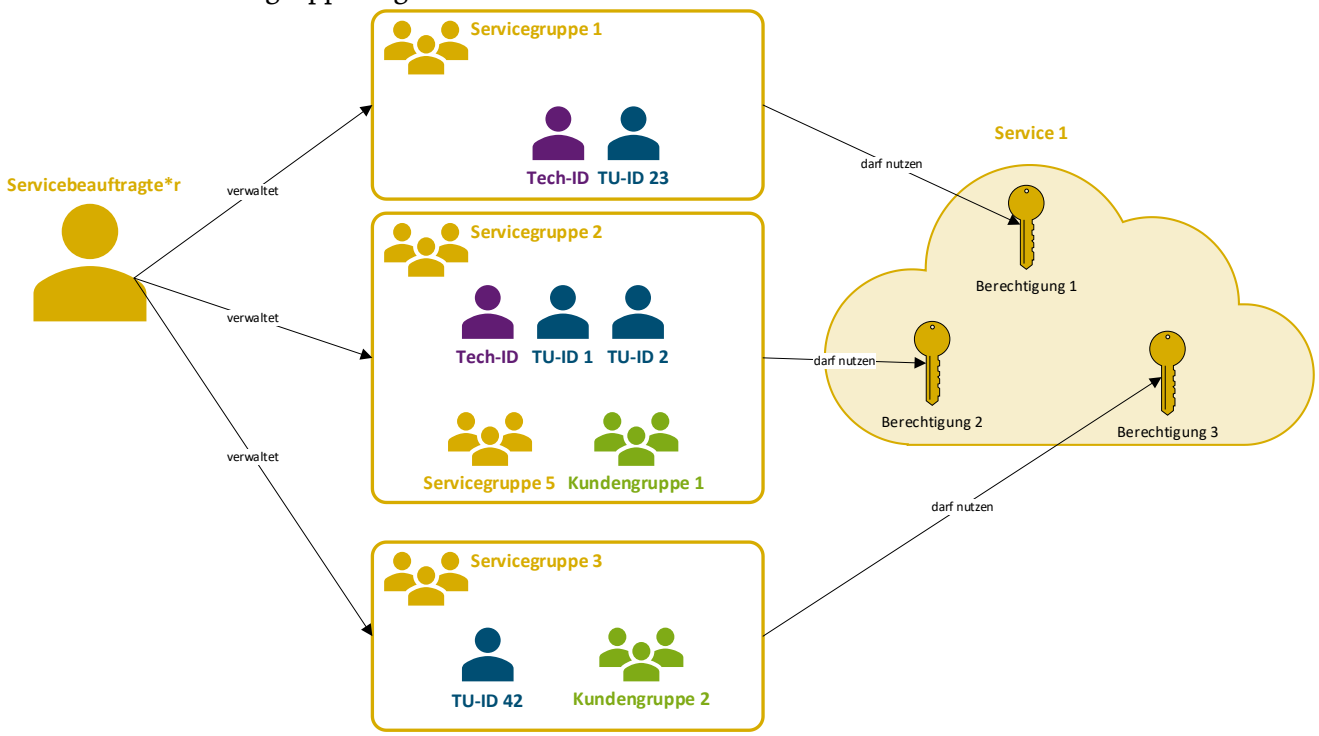

Diagramm3: Servicegruppen

4.2.3. Gruppenbeauftragte

Gruppenbeauftragte sind für die Zuordnung und Pflege von Gruppenmitgliedern in Kundengruppen zuständig. Die Kundengruppen wurden vom Kundenbeauftragten erstellt.
Der Gruppenbeauftragte trifft die Zuordnung zu diesen Gruppen.

Hier können wie bei den Servicebeauftragten folgende Zuordnungen getroffen werden:

- Einzelne Personen anhand ihrer TU-ID
- TechIDs
- Kundengruppen (Schachtelungstiefe von 5 darf nicht überschritten werden)

können einer Servicegruppe zugeordnet werden.

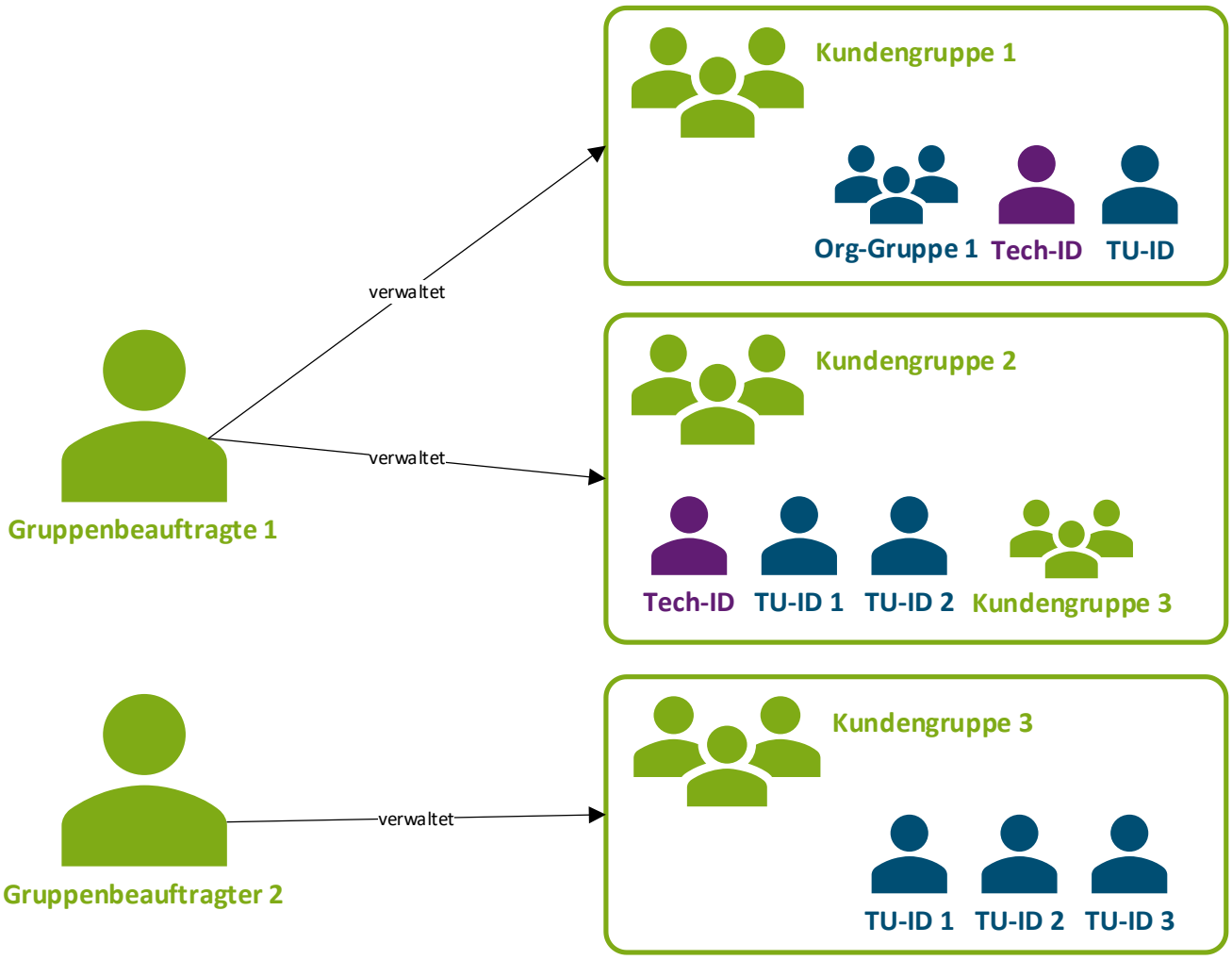

Diagramm4: Gruppenbeauftragte

5. Sicherheit

In der Gruppenverwaltung im IDM-System hat man jeweils nur Zugriff auf die eigenen Gruppen und Services.
Bei jeder Änderung (z.B. der Mitglieder) werden die betroffenen Personen informiert.
Eine Servicegruppe kann als „sicherheitsrelevant“ markiert werden. In diesem Fall werden auch die Serviceverantwortlichen informiert wenn sich Mitglieder ändern.

6. Lizenzen und Kosten

Die Gruppenverwaltung muss nicht per Lizenz erworben werden, sie ist kostenfrei und kann von den HRZ-Kund*innen via IDM Portal genutzt erstellt und zugeordnet werden.

7. Bestellen und Kündigen

7.1. Bestellen der IDM-Gruppenverwaltung

Erstellen Sie ein Ticket indem Sie zum Beispiel eine Email an den HRZ Service *service@hrz-tu-darmstadt.de* mit der Überschrift „[IDM] Teilnahme an IDM Gruppenverwaltung anfordern“ schicken.

7.2. Kündigung der IDM-Gruppenverwaltung

Erstellen Sie ein Ticket indem Sie eine Email an den HRZ Service *service@hrz-tu-darmstadt.de* mit der Überschrift „[IDM] Teilnahme an IDM Gruppenverwaltung kündigen“ schicken. Dann werden alle ihre erstellten Gruppen gelöscht.

***Hinweis**: Vorsicht diese Maßnahme ist weitreichend für die Benutzung ihrer Services, wenn die Berechtigung der Services den IDM Gruppen zugeordnet ist.*

---

8. Support

8.1. Standardwege für Supportanfragen

Supportanfragen richten Sie bitte an den HRZ Service[1)] :
Webformular: http://www.hrz.tu-darmstadt.de/kontaktformular
E-Mail: service@hrz.tu-darmstadt.de
Hotline: +49 6151 16-71 112

[1)] Es gelten die Allgemeinen Betriebs- und Servicezeiten des HRZ

9. Beispiel

9.1. Beauftragung eines HRZ Service durch einen Kunden

In diesem Beispiel möchte ein Fachgebiet im Campus den Service Sharepoint des HRZ nutzen.
Dazu kontaktiert die Kundin zunächst das HRZ und klärt ab welche Funktionen genau benötigt werden und wie die Zugriffe auf diese Funktionen eingeschränkt werden sollen. Meistens werden die Zugriffe anhand von organisatorischen Rollen eingeschränkt. Zum Beispiel gewisse Rechte für die Fachgebietsleitung und andere für die Teamassistenz.
Die Sharepoint-Administration konfiguriert dann zunächst die Sharepoint-Seiten entsprechend. Anschließend erstellt diese die entsprechenden Servicegruppen und weist diesen Rechte im Sharepoint zu.
Sollte das der erste Service des Fachgebiets sein muss das Fachgebiet zunächst als Kunde im IDM eingetragen werden. Dazu kontaktiert die zuständige Person das HRZ und bittet um Freischaltung. Der Kunde benennt mindestens zwei Kundenbeauftragte (z.B. den zentralen Admin des Fachgebiets und die Fachgebietsleitung als Backup). Diese beiden zukünftigen Kundenbeauftragten besuchen die

Schulung „Kundenbeauftragte im IDM-System“. Anschließend wird der Kunde im IDM angelegt und sie als Kundenbeauftragte zugewiesen.
Diese Kundenbauftragten erstellen für die Rollen im Team entsprechende Kundengruppen und weisen ihnen die Gruppenbeauftragten zur Pflege zu. Das wäre in diesem Beispiel die Fachgebietsleitung.
Im letzten Schritt teilt die Kund*in den Sharepoint-Admins die Namen der Kundengruppen mit. Diese können dann die Kundengruppen in die Servicegruppen einfügen.
Wenn jetzt die Fachgebietsleitung Personen in die Kundengruppen hinzufügt sind diese automatisch berechtigt.

9.2. Betrieb eines eigenen Kundenservices

Neben den Services des HRZ nutzt das oben genannte Fachgebiet auch einen selbst betriebenen Fileserver. Auch dessen Rechte sollen in Zukunft über die Gruppenverwaltung gesteuert werden.
Einer der Kundenbeauftragten erstellt dafür im IDM-Portal den Service und weist den für die Fileserver zuständigen Administrator*in als Servicebeauftragte zu.
Diese Administrator*in kontaktiert jetzt wiederum das HRZ mit der Bitte der Anbindung ihres Service an einen Authentifizierungsdienst. In diesem Beispiel wird der Fileserver per SSO angebunden.
Nach erfolgreicher Anbindung erstellt die Administrator*in die nötigen Ordnerstrukturen im Fileserver. Einen Ordner für Fachgebietsleitung und einen für die Teamassistenz. Sie legt im IDM-Portal zwei Servicegruppen an und weist im Fileserver diesen Servicegruppen Rechte an den Ordnern zu.
Anschließend fügt sie die entsprechenden Kundengruppen in die Servicegruppen ein.

9.3. Berechtigen einer neuen Person

Wenn jetzt eine neue Person zur Teamassistenz hinzukommt, muss diese von der Fachgebietsleitung nur noch in eine Kundengruppe hinzugefügt werden und hat automatisch Rechte sowohl am Sharepoint als auch am Fileserver.

10. Anhang

Nachfolgend eine Übersicht wichtiger Dokumente und Weblinks:
Informationen, Anleitungen, FAQs

- https://www.hrz.tu-darmstadt.de/*tuid*

Allgemeine Service- und Betriebszeiten

- https://www.hrz.tu-darmstadt.de/betrieb-servicezeiten

Benutzungsordnung für IT-Systeme der Technischen Universität Darmstadt

- https://www.hrz.tu-darmstadt.de/it-benutzungsordnung

IT-Sicherheitsrichtlinien (IT-Security-Policy) der TU Darmstadt

- http://www.hrz.tu-darmstadt.de/itsecurity_policy

Glossar

Begriff	Erklärung
TU Angehörige	Personen die eine gültige TU-ID haben • Beschäftigte der TU • Studierende • Gäste und Partner*innen (mit TU-ID) • Lehrbeauftragte • Studentische Hilfskräfte • Externe/Gäste (ohne TU-ID)

Kundenbeauftragte Person	Kundenbeauftragte sind für die Erstellung von Kundengruppen und Services zuständig und verantwortlich. Sie sind erste Ansprechpartner des HRZ bei Fragen zu Objekten des Kunden.
Servicebeauftragte Person	Die Servicebeauftragten erstellen die Servicegruppen und verknüpfen sie mit Rechten in ihrem Service.
Gruppenbeauftragte Person	Gruppenbeauftragte pflegen die Mitglieder von Kundengruppen.