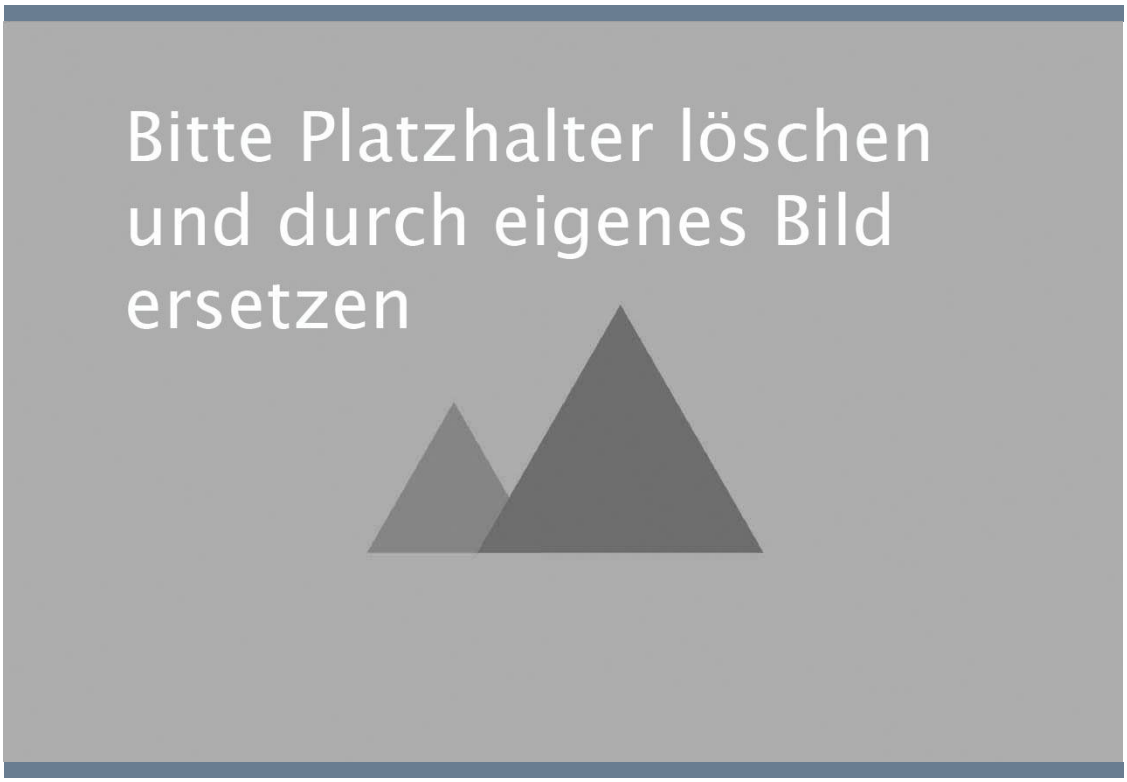

Anforderungsspezifikation <Webbasiertes Reporting von Userberechtigungen für Windows Active Directory - WRAD>

Projektteam 2/3
Dario Furigo
Philipp Köfer
Nicola Michaelis
Beat Schärz

v0.5
09.10.2018

Berner Fachhochschule
Departement für Technik und Informatik

Inhaltsverzeichnis

1 Versionskontrolle

Version	Datum	Beschreibung	Autor
0.1	28.09.2018	Dokument erstellt	N.M.
0.2	06.10.2018	Dokument erweitert (Kapitel 7.1 und 7.2)	B.S.
0.3	07.10.2018	Dokument erweitert (Kapitel 6)	D.F.
0.4	07.10.2018	Dokument erweitert (Kapitel 7.3 und 7.4)	N.M.
0.5	09.10.2018	Dokument reviewed und korrigiert	D.F.

2 Zweck des Dokuments

Dieses Dokument beschreibt die Ziele und Anforderungen für das Projekt „Webbasiertes Reporting von Userberechtigungen für Windows Active Directory

3 Vision

Das Reportingtool ist eine webbasierte Lösung, welches Audits über ein Active Directory vereinfacht. Die Lösung ist sowohl für Systemadministratoren als auch für Manager und Auditoren nützlich. Mit den Reports werden einerseits klassische Probleme wie z.B. verwaiste Accounts ersichtlich, andererseits ist aber auch ein IST/SOLL Vergleich der Berechtigungen möglich. Weiter kann dem Tool auch eine „History“ eines Users entnommen werden, welche aufzeigt wie sich dieser User über die Zeit entwickelt hat.

4 Stakeholder

Stakeholder	Beschreibung
Auditor	Der Auditor hat eine Read-Only Sicht auf die Applikation. Für ihn ist das Reporting relevant.
Systemadministrator	Der Systemadministrator hat eine Read-Only Sicht auf die Applikation. Für ihn ist das Dashboard relevant.
Application Owner	Betreibt die Applikation und hat vollen Zugriff auf das System.
Autorisierungsstelle	Prüft den SOLL Zustand und meldet Verstösse beim SOLL Zustand, wie auch beim IST/SOLL Vergleich.
Abteilungsleitung	Erfasst den SOLL Zustand und kann diesen gegen den IST Zustand abgleichen.
Auftraggeber (Christof Jungo)	Experte für das Projekt.
Projektteam	Entwickler des Projekts.

5 Projektziele

5.1 Alle Stakeholder

Es ist das Ziel ein Webservice anzubieten, welcher den IST- und SOLL-Zustand eines Active Directorys aufzeigt und verschiedene Reports generiert.
Zudem soll die Applikation dem User ein übersichtliches Dashboard zur Verfügung stellen.

5.2 Auditor

Der Auditor ist dafür zuständig, dass Normen und Gesetzgebung eingehalten werden.
Er kann einen Report generieren lassen, welcher ihm ermöglicht den Zustand des Active Directorys zu bewerten.
Der Auditor hat weder auf den IST- noch auf den SOLL-Zustand Zugriff sondern darf lediglich vordefinierte Reports ausführen.

5.3 Systemadministrator

Der Systemadministrator hat zusätzlich zum Dashboard die gleiche Sicht wie der Auditor. Er sieht so tagesaktuell Abweichung zwischen dem IST- und SOLL-Zustand seiner Objekte im Active Directory.

5.4 Application Owner

Der Application Owner hat Zugriff auf alle Einstellungen des Systems. Auf dem Dashboard müssen relevante Statusinformationen zum System ersichtlich sein. Der Application Owner stellt jederzeit die Verfügbarkeit der Applikation sicher und passt diese kontinuierlich an.

5.5 Autorisierungsstelle

Die Autorisierungsstelle prüft den SOLL Zustand, kann Reports erstellen und diese ausführen.
Auf dem Dashboard ist der IST/SOLL-Vergleich ersichtlich.

5.6 Abteilungsleitung

Die Abteilungsleitung bearbeitet den SOLL-Zustand.
Auf dem Dashboard ist primär der IST/SOLL-Vergleich ersichtlich.

5.7 Auftraggeber

Die Applikation soll ohne negative Einwirkung auf das vorgegebene System installiert werden können.

5.8 Projektteam

Ist verantwortlich für die Durchführung des Projektes und das Erreichen der gesteckten Projektziele.

6 Systemabgrenzung

6.1 Prozessumfeld

Die Applikation unterstützt die folgenden Geschäftsprozesse:
- Eintritt eines neuen Mitarbeiters und dessen Rechteverwaltung
- Austritt eines Mitarbeiters
- Mutation/Übertritt eines Mitarbeiters
- Korrektur von nichtautorisierten Berechtigungen durch den IST- und SOLL-Vergleich

Das Grundsätzliche Prozedere eines Eintrittes ist wie folgt:
Die HR-Abteilung stösst den Eintritt eines neuen Mitarbeiters an. Anschliessend wird die zuständige Abteilungsleitung des neuen Mitarbeiters das Rollenprofil bzw. die Berechtigungen festlegen (SOLL Profil). Diese Rollen und Berechtigungen werden der Autorisierungsstelle vorgelegt, welche diese prüft und freigibt. Die Autorisierungsstelle gibt anschliessend das Go für die Umsetzung an die Systemadministratoren des Active Directory als SOLL Profil oder meldet der Abteilungsleitung, dass zu viele Rollen/Berechtigungen vorhanden sind. Die Systemadministratoren informieren nach der erfolgreichen Umsetzung die zuständige Abteilungsleitung bzw. dem neuen Benutzer, dass dies geschehen ist.
Die Systemadministratoren erfassen somit den IST-Zustand im Active Directory, welcher anschliessend ausgelesen wird.

Bei einem Austritt informiert die HR-Abteilung direkt die Systemadministrator, welchen diesen User sperren und parallel dazu wird derselbe Prozess durchlaufen, um den SOLL-Zustand zu bereinigen und den User aus dem Active Directory anschliessend zu löschen.

Ein Übertritt oder eine Mutation läuft wie ein Eintritt ab, nur muss dabei die vorherige Abteilungsleitung, wie auch die neue Abteilungsleitung informiert und das SOLL angepasst werden.

Eine Korrektur von nichtautorisierten Berechtigungen bzw. einen Fehler im SOLL/IST Vergleich meldet der Auditor der Abteilungsleitung und der Autorisierungsstelle, um gegebenfalls das SOLL oder das Active Directory zu korrigieren.

Diese Prozesse unterscheiden sich natürlich von Firma zu Firma und es werden teilweise Stakeholder zusammengefasst. Autorisierungsstelle und Auditor oder Autorisierungsstelle und Abteilungsleitung können ein und dieselbe Person sein.

Der Prozess mit Ressourcen wie Sitzungszimmer, Service Accounts und Mailaccounts, welche oftmals in einem Audit als inaktiv auftauchen, ist nicht im Scope und wird direkt bei der Autorisierungsstelle abgehandelt, welche diese Accounts rausfiltern kann.
Weiterhin ist der Prüfungsmechanismus der Autorisierungsstelle nicht Bestandteil der Applikation.

Damit nach der Installation der Applikation der SOLL-Zustand einfach abgebildet werden kann, ist es für den Application Owner möglich ein CSV mit dem SOLL-Zustand nach vorgegebenem Format hochzuladen.
Alle Aktionen, die am SOLL verändert werden oder Filter, die gesetzt werden, werden protokolliert und sind nachvollziehbar vorhanden.