Design und Implementation einer rollenbasierten Zugriffskontrolle (Role Based Access Control)

Studiengang: MAS Information Technology

Das Ziel der Arbeit ist aufzuzeigen, wie die geeignetste Lösung für die Geschäftsstelle des Schweizerischen Roten Kreuz eines «Zuweisungsmodell» um Berechtigungen und Zugriffe in eine rollenbasierte Zugriffssteuerung zu provisionieren, aussehen soll. Nach dem Grundsatz von Berechtigungen, so viel wie nötig, so wenig wie möglich.

Einleitung

Zurzeit existiert kein etabliertes Identity- und Access-Management (IAM). Der Aufwand für die Bewirtschaftung des «User Lifecycle Managements» ist sehr hoch. Alle Änderungen von Berechtigungen und Zugriffen werden durch das IT Fachpersonal manuell vorgenommen. Neue User-Accounts werden vom Vorgänger oder einem anderen Account im gleichen Team kopiert und umbenannt. Dieser Prozess provoziert Fehler, weil die Berechtigungen in allen Systemen und Applikationen manuell vorgenommen werden.

Datenanalyse/Recherche

Die Daten werden aus unterschiedlichen Quellsystemen erhoben. Analysiert wurden die definierten Applikationen sowie das Microsoft Active Directory. Auch die Funktionsbeschreibungen und Organigramme werden in der Analyse und Recherche mit einbezogen, um das Gesamtbild zu vervollständigen. Die analysierten Daten werden, sofern ein Mehrwert entsteht, zusammengeführt oder ergänzt und mit zusätzlichen Informationen angereichert.

Vorgehen/Methodik

- Festlegung der Standard-Berechtigungen, über welche alle Mitarbeitenden der GS SRK verfügen
- Zuweisung der Organisatorischen-Berechtigungen, welche die Departements-spezifischen Berechtigungen beinhalten
- Den Funktionalen-Berechtigungen, welche die Ausübung der Funktion (Rolle) des Mitarbeitenden sicherstellt
- Letztendlich werden die Spezial-Berechtigungen der Rolle zugewiesen, welche der Mitarbeitende zur Ausübung einer oder mehrerer Sonderfunktionen benötigt

Massnahmen

- Stellenbezeichnung in der Personal Management Applikation Rexx müssen geregelt werden
- Bereinigung des Microsoft Active Directory von den Altlasten inklusive eines Konzepts mit den standardisierten Vorgaben für die Verwendung
- Vertiefte Analyse der Berechtigungen in den Business-Applikationen
- Vorgesetzten Interviews zur Verifizierung der Berechtigungen der Mitarbeitenden
- Definition des Bestätigungs- oder Bescheinigungsprozesses

Ergebnis

Diese Massnahmen führen zum Ziel dieser Arbeit, der Etablierung eines «Zuweisungsmodells» für die Berechtigungen und Zugriffe einer rollenbasierten Zugriffssteuerung innerhalb der GS SRK.

Patrick Neff

Übersicht der Basisberechtigungen (Birth Rights)

| Business-Rollen | Berechtigungs-Gruppen | | |