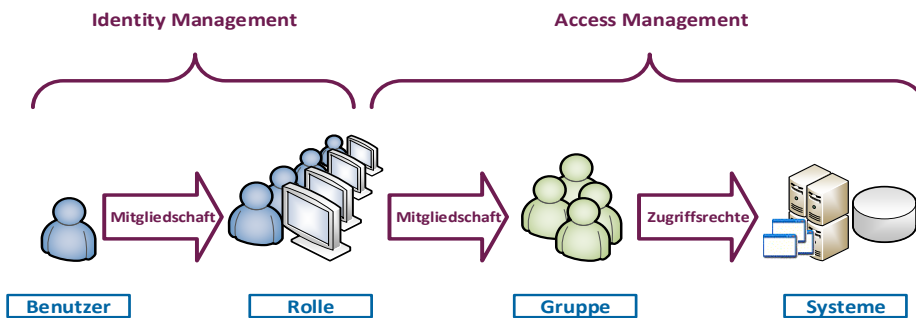


Identity und Access Management an der HSR

An der HSR hat jeder Mitarbeiter und jeder Studierende mindestens eine elektronische Identität in Form eines Benutzer-Accounts für die Systeme der HSR. Mit diesem Benutzer-Account kann er spezifisch auf die Systeme der HSR zugreifen und wird als berechtigter Nutzer wahrgenommen.

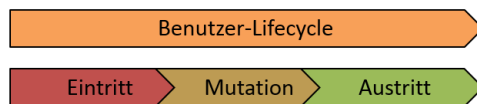


Das Ziel von IAM ist es, allen Benutzern abhängig von den Rollen, welche sie an der HSR wahrnehmen, genau diejenigen Berechtigungen zu gewähren, welche für ihre Arbeit oder das Studium notwendig sind.

Dafür hat IAM Schnittstellen zum ActiveDirectory und zu den wichtigsten IT Anwendungen der HSR.

Benutzer-Lifecycle

Das Bachelorstudium an einer Fachhochschule dauert durchschnittlich 3,3 Jahre¹. Es werden also jedes Jahr ca. 1/3 der Studierenden-Accounts gelöscht und durch neue ersetzt. Dazu kommen noch Accounts für Dozierende, Mitarbeiter, Master- und Weiterbildungsstudierende. Die Accounts werden im Rahmen der bestehenden Eintrittsprozesse erzeugt und in den Austrittsprozessen deaktiviert. 5'500 Mutationen werden im Verlaufe eines Jahres über IAM verarbeitet.

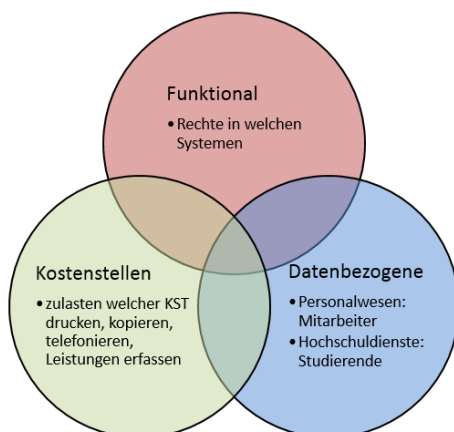


Durch die Einbindung von IAM in die Geschäftsprozesse kann sichergestellt werden, dass mit jedem Eintritt der Benutzer-Account erstellt wird und mit dem Austritt auch die elektronische Identität endet.

IAM beinhaltet dafür eine Workflow-Engine, welche die Accounts im ActiveDirectory erstellt und auch wieder löscht, sowie die betroffenen administrativen Stellen über notwendige Aktivitäten informiert.

Berechtigungssteuerung

IAM bildet alle wichtigen Rollen, die eine Person an der HSR wahrnimmt in seiner Datenbank ab.



- Die Berechtigungen, welche eine Person zu einem bestimmten Zeitpunkt hat oder hatte (Historisierung) sind jederzeit und vollständig nachvollziehbar.
- Kostenstellen-Zuordnungen regeln den Bezug von Leistungen zulasten von Kostenstellen, z.B. Druckkosten (CANON UniFLOW) oder Bezüge von Büromaterial.
- Die Zutrittsberechtigung zu den Gebäuden wird (über den persönlichen Badge des Benutzers) von IAM aus gesteuert.
- Die Umsysteme nutzen die Informationen in IAM über definierte, automatisierte Schnittstellen um ihre funktionalen und datenbezogenen (Rowlevel Security) Berechtigungen zu steuern.
- Scripts steuern mit dem Input aus IAM die Berechtigungen über Gruppenzuteilungen im ActiveDirectory der HSR.

Neben den persönlichen Accounts als primäre elektronische Identität, werden Zusatz- Accounts sowie unpersönliche Accounts für Organisationseinheiten, Services, Tests etc. unterstützt.

„Mit Hilfe von IAM haben die Verantwortlichen der HSR immer den Überblick über die Personen mit ihren elektronischen Identitäten. Es ist nachvollziehbar, welche Systeme diese nutzen können und sicher, dass die Berechtigungen gelöscht werden, wenn die Personen austreten oder ihre Funktion ändern. **IAM ist ein wichtiges Instrument für das IT Controlling und ganz im Sinne der IT Revision**“

Hans-Peter Egli, Verwaltungsdirektor HSR

¹ Quelle: Bundesamt für Statistik, Studiendauer an den FH und PH 2012