Einfluss der Digitalisierung auf Identity- & Access-Management-Systeme

Innovationen in der Informations- und Telekommunikations-Technologie führten in den letzten Jahren dazu, dass Online-Dienste weitverbreitet und allgegenwärtig im Alltag der Menschen geworden sind. Die Evolution des Internets von einem Medium der reinen Informationsbereitstellung hin zu einer interaktiven Plattform, ermöglicht die Nutzung von diversen personalisierten Services im Bereich E-Commerce sowie zahlreichen anderen Diensten. Das Interesse am Identity- & Access-Management (IAM) ist darauf zurückzuführen, dass Identitäten und die darin enthaltenen personen- sowie maschinenbezogenen Informationen einen hohen kommerziellen Wert besitzen. Das IAM stellt damit einen wesentlichen Bestandteil für die Entwicklung der „Internet-Economy" dar und führt zu nachhaltigen Wertbeiträgen, indem es die Sicherheit erhöht und die Verwaltung von Identitäten vereinfacht.

1 Identity- & Access-Management (IAM)

Der Begriff Identity- & Access-Management wird in Literatur und Praxis häufig als Modewort genutzt, kann jedoch unterschiedliche Bedeutungen haben:[1]

- *Enterprise-IAM: Die Verwaltung von Konten von Mitarbeitern, Kunden oder Bürgern. Diese Konten enthalten die Bestandteile einer Identität, die relevant für eine Institution bzw. ein Unternehmen sind (bspw. Attribute, Rollen etc.)*
- *Consumer-IAM: Die Möglichkeit einer Person, ihre verschiedenen Teilidentitäten mit den verschiedenen Unternehmen zu verwalten.*
- *Machine-IAM: Machine-IAM ermöglicht es, dass Maschinen, Geräte und „Dinge" sich anhand verschiedener Identitätskonzepte gegenseitig authentifizieren und autorisieren können. Dies stellt einen essentiellen Faktor bei der technischen Umsetzung von „Internet of Things"- und „Machine-to-Machine"-Kommunikation dar.*

Die einzelnen Kernfunktionalitäten eines IAM-Systems sind in der Abbildung 1 dargestellt. Das Framework berücksichtigt alle relevanten Funktionen eines IAM-Systems, die es ermöglichen, Identitäten über den gesamten „Identitätslebenszyklus", von der Speicherung der Anwenderdaten über die Authentifizierungs- und Autorisierungsprozesse bis hin zur Bereitstellung einer einheitlichen Benutzeroberfläche, zu verwalten.

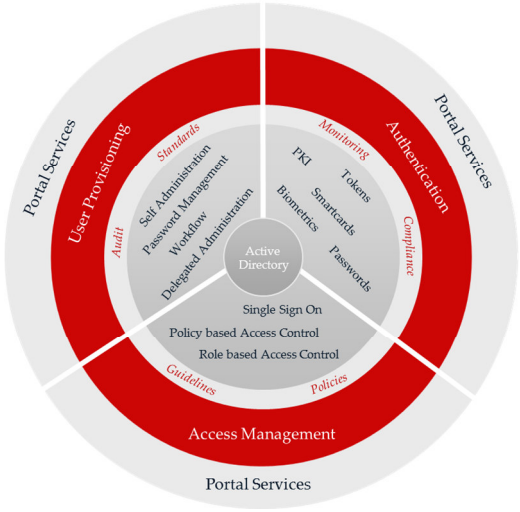

Abbildung 1: IAM-Framework (in Anlehnung an[2])

2 „IAM 4.0": Rolle im digitalen Zeitalter

Während Unternehmen früher ihr stets knappes IT-Budget dahingehend planten, ausschließlich technische Probleme zu lösen, so handelt es sich in der heutigen modernen Informationsgesellschaft viel mehr um eine „Business-enabling IT", d. h. innovative IT-Lösungen werden eingesetzt, um „Business" zu ermöglichen und voranzutreiben. Dies ist auch zwingend notwendig, denn die heutigen Geschäftsmodelle haben sich mit dem technischen Fortschritt und der zunehmenden Digitalisierung enorm gewandelt. Endkunden werden verstärkt über personalisierte Online-Zugänge akquiriert bzw. an das Unternehmen gebunden. Das IAM hat bei der Entwicklung der IT-Rolle eine besondere Bedeutung, da es einen nachhaltigen Wertbeitrag mit greifbaren Vorteilen leistet. Es schafft eine vertrauensbasierte Beziehung zwischen den beteiligten Parteien, bspw. zwischen einem Online-Einkäufer und einem Online-Händler, und stellt damit die Grundlage für die Realisierung von identitätsbasierten Geschäftsmodellen. Damit geht das „IAM 4.0" über die klassische Bedeutung des IAMs hinaus, indem es Unternehmen dabei unterstützt, nachhaltige Kundenbeziehungen aufzubauen, ihre Produkte und Services zu verbessern und diese gezielter und effektiver anzubieten. Weiterhin bietet es mit Modellen wie Federated IAM oder Social Login optimale Voraussetzungen für die Einbindung von Geschäftspartnern und Kunden.

3 Herausforderungen von IAM

Inmitten der heiß diskutierten Hype-Themen wie „Industrie 4.0“ und „Internet of Things“ müssen neben den Maschinen, Geräten und Software-Anwendungen insbesondere die Nutzer dieser Technologien betrachtet werden, denn mit der Digitalisierung und Automatisierung nehmen auch die Risiken des Datenmissbrauchs und Identitätsdiebstahls zu. Ein sicheres IAM wird in diesem Zusammenhang als unabdinglich eingestuft.

User nutzen das Internet bspw. um ihre Finanzen zu verwalten, auf E-Commerce-Plattformen einzukaufen oder in sozialen Netzwerken miteinander zu kommunizieren. Jede dieser Anwendungen erfordert die Erstellung eines Kontos, einer sog. „digitalen Identität“. Damit werden Nutzer mit zahlreichen Authentifizierungsmechanismen konfrontiert, denn eine digitale Identität benötigt stets ein Berechtigungsnachweis wie bspw. Zugangsdaten in Form einer Nutzername-Passwort-Kombination. Hierbei gilt es den Überblick über eine Vielzahl von Login-Daten zu behalten und diese nach dem Grundsatz einer hohen Sicherheit zu erstellen und in regelmäßigen Zeitabständen zu erneuern. Mit der zunehmenden Nutzung von verschiedenen identitätsbasierten Services, steigt damit die Komplexität hinsichtlich der Verwaltung der digitalen Identitäten. Wie in der Abbildung 2 dargestellt, ergeben sich drei wesentliche Herausforderungsbereiche: Informationssicherheit, Privatsphäre und Benutzerfreundlichkeit.

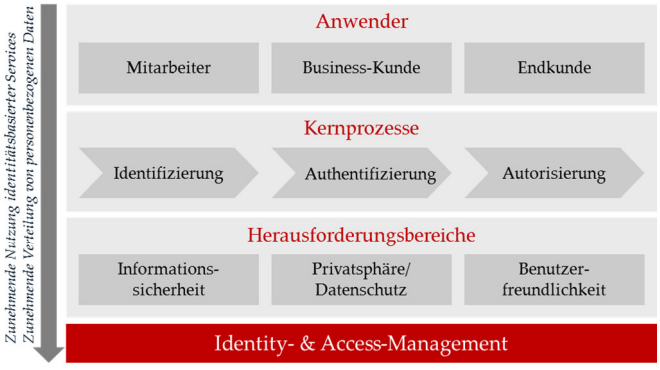

Abbildung 2: Grundproblemstellung digitaler Identitäten

4 Die HDP als Partner im IAM-Umfeld

Auch wenn die meisten IT-Entscheider IAM als wichtig erachten, ist häufig die Geschäftsführung noch nicht davon überzeugt. Fakt ist jedoch, dass unzählige Identitäten und Zugriffsberechtigungen verwaltet und immer dynamischer gestaltet werden müssen. Dabei sehen sich Unternehmen immer mehr den Herausforderungen des digitalen Wandels und der Aufgabe gegenüber, einen benutzerfreundlichen und vor allem sicheren Identitätslebenszyklus, verstärkt auch in öffentlichen Cloud-Infrastrukturen sowie Industrie 4.0-Umgebungen, zu gewährleisten. Möglichst einfache und intuitive Registrierungsprozesse sowie ein vertrauenswürdiger, sicherer und gesetzeskonformer Umgang mit Identitäten jeglicher Art sind daher zwingende Voraussetzungen, um das Vertrauen von Mitarbeitern, Kunden und Partnern langfristig sicherzustellen.

Die HDP bietet hierfür ein umfassendes Leistungspaket basierend auf ein bereits mehrfach eingesetztes HDP-IAM-Framework an (Abbildung 3):

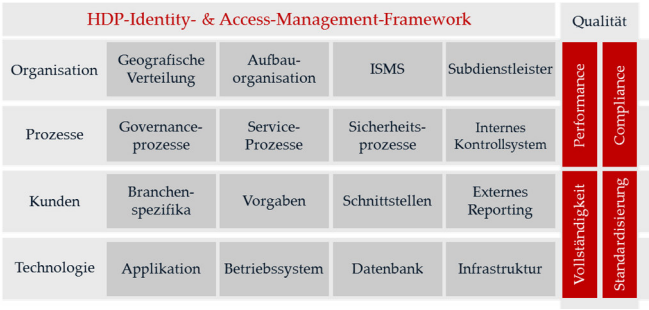

Abbildung 3: HDP-IAM-Framework

Darauf aufbauend berät die HDP den vollständigen IAM-Prozess von der Prozessoptimierung bis hin zur Bewertung, Auswahl und Implementierung einer zielführenden und strategiekonformen IAM-Lösung. Konkret heißt das, wir unterstützen unsere Kunden auf Basis unserer Projekt-Erfahrungen in der Aufnahme der individuellen Anforderungen an ein IAM, der aktuellen Prozesse und deren Reifegrad sowie bei der Bewertung der Risiken. Anschließend optimieren wir die relevanten Prozesse und helfen bei der Auswahl des richtigen Tools durch die Entwicklung von kundenindividuellen Use-Cases zur Toolbewertung und den Vertragsverhandlungen hinsichtlich Lizenzen, Wartung und dem Implementierungsprojekt.

Literatur:

[1] in Anlehnung an *Rannenberg, Kai:* Identity Management 1, Information & Communication Security, Lecture 7. WS2012/2013, Goethe-Universität, Frankfurt am Main

[2] *Vanamali, Srinivasan:* Identity Management Framework-Deliver Value for Business. Information Systems Control Journal, Volume 4 (2004), Information Systems Audit and Control Association