smf
YOUR IT PARTNER

# IDENTITY & ACCESS MANAGEMENT

## Herausforderungen und Chancen in der Digitalen Transformation

# INHALT




Autor: Phillip Conrad, SMF GmbH


Stand: 03.03.2021

# IDENTITY & ACCESS MANAGEMENT

## HERAUSFORDERUNGEN UND CHANCEN IN DER DIGITALEN TRANSFORMATION

Welche Kunden, Mitarbeiter, Partner und Lieferanten sind mit welchen Rechten und Daten in Ihrer IT-Infrastruktur unterwegs? Eine Herausforderung ist diese Frage für jeden IT-Verantwortlichen allemal. Nicht selten aber auch eine Überforderung. Dabei ist die Notwendigkeit, die Digitale Transformation (DT) nicht nur massiv voranzutreiben, sondern auch abzusichern, so drängend wie nie: Vertrauliche Daten, die zwischen immer mehr Services herumgereicht werden, sind kein neues Problem mehr. Externe Cloud-Services, Remote-Arbeit, Home-Office, Geschäftsprozesse ohne persönlichen Kontakt – all das ist im Begriff, sich zu etablieren. Im Umfeld der Rollen- und Rechteverteilung (Identity and Access Management – kurz: IAM) sollte also verbindliche Klarheit herrschen, um dauerhaft die notwendigen Sicherheits- und Compliance-Richtlinien im Griff zu behalten.

Zu jeder DT-Strategie gehört eine tragfähige und ganzheitliche IAM-Lösung. Denn der frühere Sicherheitszaun, der Anwendungen im Intranet oder in der sogenannten entmilitarisierten Zone (DMZ) isoliert hat, steht der DT schlicht im Weg. Umfassende Kommunikation mit externen Partnern, die z. B. auf eigene Services zugreifen sollen – diese Möglichkeiten lässt der Zaun nicht zu. Als Plattform braucht es das offene und somit grundsätzlich unsichere Internet.

Derzeit sichere Passwörter sollten mindestens 20 Stellen haben, Tendenz steigend. Die ständig irgendwo einzugeben ist a) aufwändig, verleitet b) zu nicht ratsamen einfachen Passwörtern, vergrault c) Kunden, erhöht d) die Chance, dass Passwörter abgefangen werden und ist e) unterm Strich somit keine echte Lösung. Ein Single-Sign-On, wie wir es im Consumer-Markt von Google oder Facebook kennen, wird in den kommenden Jahren State oft the Art sein. So entsteht nicht nur Bedarf an neuen Sicherheitsmechanismen – sondern auch nach der Reduktion der Nutzerkontenmenge pro Person. Die Zusammenführung aller erhaltenen Informationen zu einer digitalen Identität ist die Folge. Nur das garantiert schon heute den Komfort, den der Kunde erwartet. Und die ökonomischen Vorteile, die Unternehmen nutzen können und sollten.

## FUNKTIONIERT EIN UNTERNEHMEN LANGFRISTIG OHNE IAM?

Um es vorwegzunehmen: nein. Die Zufriedenheit der Kunden ist die Basis jedes unternehmerischen Erfolges. Und ob ein Kunde zufrieden oder unzufrieden ist, hängt in hohem Maß von der User Experience ab, die er in der digitalen Welt mit einem Unternehmen macht. Das bloße Einkaufen in einem in sich geschlossenen Shop inklusive Bezahlvorgang ist heute eine Selbstverständlichkeit. Der Anspruch steigt allerdings exponentiell, je mehr Dienste sich hinter einem Login verbergen: Kontakt ins Unternehmen hinein, Nutzung mehrerer Dienste, kundenbezogene Dienste wie Nachverfolgung von Antragsstand, Produktion und Versand, Verknüpfung mit weiteren Dienstleistern … gerade im B2B-Bereich fächert sich schnell ein komplexes Netzwerk auf. In dem, und das macht die Sache kompliziert, bei weitem nicht jeder alles wissen darf.

Ebenso wichtig ist eine intelligente DT in der internen Kommunikation. Zum einen soll die Kommunikation mit Kunden und Externen natürlich auch für alle Mitarbeiter abbildbar sein. Zum

anderen lassen sich eigene Prozesse erstellen, die die Mitarbeiterfreundlichkeit durch intelligente Automatismen und Vorverarbeitungen verbessern. Durch sogenannte Robotic Process Automation etwa können wertvolle Personalressourcen von eintönigen und zeitintensiven Prozessschritten abgezogen werden.

Durch die DT wird die Zusammenarbeit zwischen unterschiedlichen Abteilungen und über Unternehmensgrenzen hinweg effizienter, reibungsloser und deutlich weniger anfällig für Fehler. Zudem werden sämtliche Prozesse vollständig transparent – vertrauensbildend für Kunden und Geschäftspartner, hilfreich bei Identifizierung von Fehlerquellen.

Ein erster Meilenstein auf dem Weg zu diesem Ziel ist die Etablierung digitaler Schnittstellen zwischen den verschiedenen Parteien (z. B. Kunden und Mitarbeitern). Allein das ist undenkbar ohne IAM: Wie weisen sich die Nutzer aus? Ist die Nutzeridentität bereits vorhanden? Übersteigt die Menge an neuen Nutzerkonten die Verwaltungskapazitäten? Wie wird ermöglicht, die gleiche Identität in unterschiedlichen Diensten zu nutzen? Braucht es dazu weitere Daten des Nutzers? Braucht es weitere Lizenzen? Welche Nutzerdaten braucht es in welchen Prozessen? Und welche nicht?

Die Erfahrung zeigt, dass die Zahl der Fragen im Verlauf der Umsetzung ständig zunimmt. Die Erfahrung zeigt auch, dass Unternehmen und Verwaltungen mitunter kapitulieren und den fatalen Weg zurück zum Sicherheitszaun gehen. Schon heute ist das ein Innovationshindernis und Wettbewerbsnachteil. Schlimmer noch: Improvisierte Teillösungen führen zu Compliance- und Rechts-Verletzungen, ebenso zu Hochlast bei der IT-Abteilung und damit zu Fehlern und Unzufriedenheit. Um das zu vermeiden, hilft es, im Zuge der DT einen zentralen IAM-Dienst zu etablieren.

## WIE KÖNNEN FACHLICHE ANFORDERUNGEN AN EINE IAM-LÖSUNG AUSSEHEN?

Ein immer wiederkehrender Aspekt: die Entlastung des Helpdesks aufgrund steigender Nutzerzahlen. Keinesfalls darf die DT beim IAM-System selbst stoppen. Self-service-Funktion bei Registrierung oder Passwortwiederherstellung sowie Antragsprozesse rund um Rechteanfragen und ihrer Gewährung sind ohne Alternative, weil der Nutzer sie schlicht erwartet. Die Verwaltungsprozesse innerhalb der IAM-Lösung sollen durch softwaregestützte Workflows begleitet werden: Die Sachbearbeitung innerhalb des IAM soll so einfach und effizient (also ressourcenschonend) wie möglich sein. Fachabteilungen können einbezogen werden, Vorgesetzte ausgewählte Rechte selbstständig vergeben.

Ein immer wieder gemachter Fehler: die Vergabe von individuellen Rechten pro Anwendung und pro Nutzer. Das ist schon bei kleinen Nutzerzahlen zeitlich ineffizient und fehleranfällig. Hier braucht es ein Umdenken in Rollen, die gängige Arbeitsfelder und daraus resultierende Zugriffsrechte auf Softwarelösungen abbilden. Das führt sowohl zur Vereinfachung als auch zur Etablierung von wiederkehrenden Rollenprofilen. Allerdings muss diese Rollenkonstruktion exakt und differenziert genug gewählt werden. Nur so ist sichergestellt, dass niemand Zugriff auf Daten erhält, die nicht für seine Augen bestimmt sind (Least Privilege). Gerade in serviceorientierten IT-Landschaften ist dieser Aspekt wichtig. Ein IAM-Dienst kann die Datenhoheit über alle Nutzerdaten übernehmen und pro Anwendung nach den definierten Rollen steuern. Das ermöglicht die Reglementierung aller angebundenen Anwendungen und schafft insbesondere bei der Anbindung von externen Partneranwendungen zusätzliche Steuerungsmöglichkeit inklusive Sicherheit.

Ein modernes IAM weiß und regelt, welche Dienste auf welchen personenbezogenen Daten operieren. Hierdurch kann die Bearbeitung von Anfragen zur Datenauskunft oder Datenlöschung beschleunigt werden. Und ebenso die Einhaltung von Verfahrensbeschreibungen nach der DSGVO technisch durchgesetzt werden (Privacy by Design): Ein unzweckmäßiger Einsatz nicht freigegebener personenbezogener Daten wird durch eine IAM-Lösung somit zentral und sicher unterbunden.

## WIE NUTZE ICH DIGITALE IDENTITÄTEN?

Im Rahmen des IAM kann die digitale Identität eines Nutzers abgebildet werden. Bei einer technischen Betrachtung sind das neben menschlichen Nutzern auch Geräte und Services aus der IT-Landschaft. Die Identitätsdaten können zur Beantwortung von verschiedenen Fragen eingesetzt werden:

- WIE SIEHT DIE IDENTITÄT MEINES NUTZERS AUS?

Zur Verwaltung von Identitäten werden Informationen zur Identifikation zentral gesammelt und vollständig geschützt gespeichert. Dies umfasst z. B. Nutzernamen, Adressinformationen, veri-

fizierte E-Mail-Adressen, Passwörter, Standortinformationen (z. B. IP-Geolocation), biometrische Merkmale, Sicherheitsfragen sowie weitere fachkontextspezifische Nutzerinformationen. Auch vom Nutzer freiwillig gemachte Angaben können dazugehören. Durch diese Zentralisierung gehören Passwörter der Vergangenheit an, die sich auf einzelne Anwendungen beschränken. Ein mehrfaches Erfassen von Nutzerstammdaten entfällt natürlich ebenso. Die erweiterten Informationen können außerdem genutzt werden, um inhalts- oder risikoabhängig eine Mehrfaktor-Authentifizierung durchzuführen. Standortinformationen zum letzten Login helfen u. a. dabei, untypisches Verhalten zu identifizieren.

- WELCHE ZUGRIFFSRECHTE (AUCH ZUTRITTSRECHTE) BESITZEN MEINE NUTZER?

Zur Regelung des Access-Managements werden die Identitäten in erster Linie mit Rollenprofilen und Rollen (s. o.), darüber hinaus ggf. mit einzelnen Rechten verknüpft. So wird festgelegt, auf welche Systeme oder Ressourcen die Identität (der Nutzer) Zugriff erhält. Solche Rechte können bis auf Datenquellen oder Datensätze herab abgebildet werden. Dabei müssen die später angebundenen Dienste oder Anwendungen diese Rechte auch durchsetzen können.

- WELCHE LIZENZEN WERDEN VON MEINEM NUTZER VERWENDET?

Die zentrale Rechteabbildung ermöglicht es, im IAM die genutzten Softwarelizenzen zu identifizieren. Viele IAM-Lösungen bieten einen regelmäßigen Kontrollmechanismus: Hier werden die Fachabteilungen angebunden und müssen jeden Bedarf an Rechten und Lizenzen bestätigen. Und wenn sich vernetzte Softwaresysteme in automatisierten Workflows untereinander Daten zuspielen sollen, dann kann die Herkunft und Lizenzierung dieser Daten ebenfalls eine große Rolle spielen (Data Lineage).

- WO LIEGEN DIE INTERESSEN MEINER NUTZER?
- WIE SIEHT DER NUTZUNGSVERLAUF MIT MEINEN SERVICES AUS?

Willigt der Nutzer ein, sind diese Daten zur Weiterentwicklung der Geschäftsfelder oder zum interessengerechten Marketing einsetzbar. Da es sich um eine Win-win-Situation handelt, dürfen dem Nutzer durchaus die Vorteile einer solchen Einwilligung vorgestellt werden. Durch den durchgängigen Einsatz eines Nutzerkontos für alle Dienste ist ein persönlicher Fußabdruck erkennbar, welcher wiederum – ähnlich zum Geostandort – bei Abweichungen zur Intrusion-Detection eingesetzt werden kann.

## IAM IN CLOUD UND SCHATTEN-IT

Die Digitale Transformation steht für Agilität und die Beschleunigung der Prozesse. Dabei dürfen Unternehmens- und Sicherheitsrichtlinien freilich nicht ausgehebelt werden. Schatten-IT, die mit der Kreditkarte der Fachabteilung in der Cloud gebucht wird, ist der Schreck eines jeden IT-Verantwortlichen. Wie wird sichergestellt, dass die Password-Policy dort eingehalten wird? Dass aus dem Unternehmen ausscheidende Mitarbeitende sämtliche Zugriffsrechte verlieren? Übernimmt die Fachabteilung diese Verantwortung selbst, ist der Erfolg nicht garantiert, im schlimmsten Fall wurde der Bock zum Gärtner gemacht. Die Lösung für dieses Problem heißt Zero-Trust: Vertraue niemanden und verifiziere jeden. JEDE Kommunikation wird durch ein zentrales IAM authentifiziert und autorisiert. Für Services in der Cloud und im Intranet gelten die gleichen hohen Sicherheitsansprüche und werden durch das IAM durchgesetzt. Schatten-IT-Lösungen werden ebenfalls an das IAM-System angebunden und verwaltet, als wären es interne Dienste.

So steigt das Sicherheitslevel auch für die internen Anwendungen. Das ist unbedingt sinnvoll, denn die sogenannten Innentäter sind statistisch das größte Risiko für eine IT-Struktur – gern auch unbedacht und ohne Absicht. Störende Grenzen bei der Arbeit von unterwegs oder im Homeoffice entfallen auf diese Weise. Und jede webbasierte Unternehmensanwendung kann über das Internet ohne VPN-Zugänge sicher erreichbar gemacht werden.

Im Kontext der Cloud-Anbindung ist ein zentrales IAM zusätzlich von Nutzen: Werden aus lokalen und isolierten Nutzeridentitäten zentrale dienstübergreifende Nutzerkonten, ermöglicht das den störungsfreien Wechsel von On-Premise- auf Cloud-Umgebungen (und ggf. umgekehrt). Ein IAM unterstützt bei einer Cloud-Integration auch bei der notwendigen Bereinigung und Konsolidierung von Identitätsdaten. Cloud-Anbieter wie z. B. AWS, Microsoft Azure oder Google Cloud bieten in ihrem Serviceportfolio ebenfalls IAM-Komponenten an. Diese unterstützen die Rechte- und Rollendurchsetzung von Anwendungen, die auf der Cloud betrieben oder entwickelt werden. Der Fokus liegt hierbei auf der Bildung eines zentralen Nutzerverzeichnisses, das ebenfalls eine Vergabe von Rechten ermöglicht. Ungelöst bleibt hierbei allerdings die Unterstützung bei der IAM-Sachbearbeitung und Koordination des Lifecycles von Nutzerkonten, da sich diese Dienste derzeit noch überwiegend an IT-Administratoren oder Softwareentwickler richten. Fachliche IAM-Prozesse wie z. B. Workflows zum User-Lifecycle (Onboarding, Offboarding), das Passwortmanagement, die Provisionierung von Identitätsinformation an und in anderen Anwendungen, das Privacy and Consent Management sowie Audit- und Reporting-Features müssten in die IAM-Verzeichnisse der Clouds initiativ implementiert werden. Die Problematiken Vendor-Lock und Grenzen in der Kombinierbarkeit mit Diensten anderer Cloud-Anbieter bleiben ebenfalls zu berücksichtigen.

Eine flexible Lösungsarchitektur zur Verhinderung von Abhängigkeiten oder gar Redundanzen: ein losgelöstes, den Prozess unterstützendes IAM, das als führende Identitätsquelle (Identity-Provider) mit der Cloud-Infrastruktur verknüpft wird. Auf diese Weise bleiben möglich: die Werkzeug-Unterstützung bei Administrations-Aufgaben entlang des Lebenszyklus der Identität, das Einbeziehen von Fachabteilungen in den IAM-Prozess sowie generell die Verlagerung des technischen Rollen- und Berechtigungsproblems auf eine fachliche Ebene.

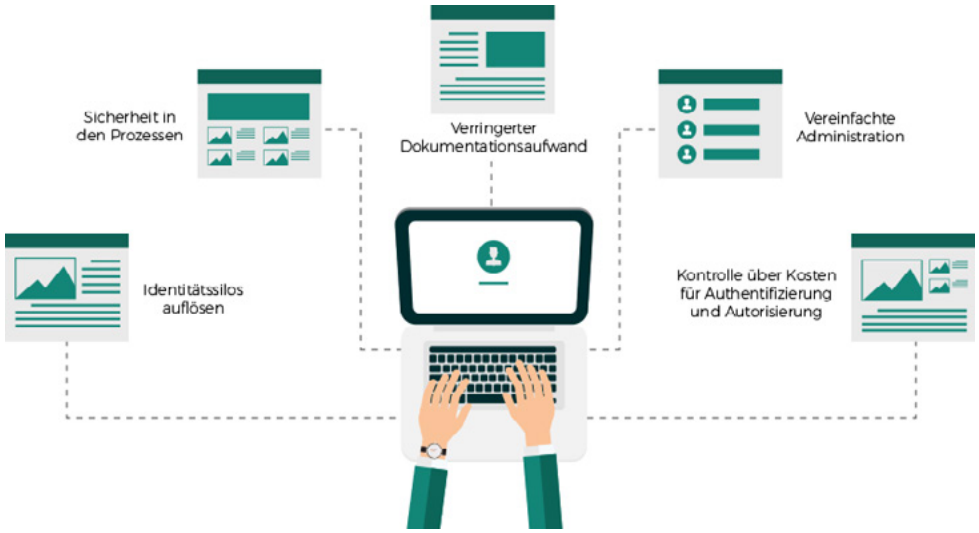
## AUF DEM WEG ZUM SINGLE-SIGN-ON

Nach der SQL-Injection als häufigstes Einfallstor bleibt die Broken Authentication das zweitgrößte Sicherheitsrisiko für Webanwendungen[1]. Dabei gelingt es den Eindringlingen, sich als rechtmäßige Nutzer auszugeben.

Aufgrund des nicht mehr vorhandenen Sicherheitszauns (inkl. VPN-Schranke) sind in einer grenzenlosen IT-Landschaft die meisten Services direkt über das Internet erreichbar. Das erfordert Vertrauen in die Sicherheit der jeweiligen Anwendungen. Die Zentralisierung aller Authentifizierungs- und Autorisierungsvorgänge durch eine IAM-Lösung erlaubt, einen Single-Point-of-Trust zu etablieren. Wird dieser ausreichend abgesichert und auf Authorisierungs-Frameworks wie z. B. OAuth2, OpenID oder WebAuthn gesetzt, können sämtliche Sicherheits-Herausforderungen für alle angebundenen Lösungen einmal zentral gelöst werden.

Das bringt die IT mit den digitalisierten Geschäftsprozessen ein ganzes Stück näher an das Architekturprinzip Security-by-Design: Denn die Sicherheitsrichtlinien auf Unternehmensarchitektur-Ebene erzwingt, dass alle Dienste den sichereren Single-Point-of-Trust einsetzen. Und diese Richtlinie zählt zu den Security-by-Design-Maßnahmen. Zur Absicherung besonders kritischer Service-Schritte lassen sich zusätzliche Funktionen wie zeitbasierte Einmal-Kennwörter (OATH-

1 Quelle: https://owasp.org/www-project-top-ten/




TOTP[2]) nutzen. Sie fungieren als Zwei-Faktor-Authentifizierungs-Mechanismen und lassen sich aus dem IAM-Portfolio in die Fachanwendungen einbinden.

All diese Authorisierungs-Frameworks reduzieren durch webbasierte Single-Sign-On-Zusammenschlüsse die Eingabe von Zugangsdaten. Das reduziert ebenfalls die Angriffsvektoren für z. B. Phishing-Attacken und regt die Nutzer – gemeinsam mit einer vorgeschlagenen Password-Policy – dazu an, ein stärkeres Passwort zu wählen, das seltener und lediglich an einer Stelle eingegeben werden muss.

## LAST BUT NOT LEAST: DIE EINHALTUNG VON REGULARIEN

Spätestens seit der EU-DSGVO bleibt kein Bereich mehr unreguliert. Es gilt zu dokumentieren, warum welche Identitäten welche Zugriffsrechte auf welche Daten und Systeme besitzen. Je nach Geschäftsfeld kommen spezifische Anwendungen hinzu. Nachfolgend nur ein kleiner Auszug:

- EU-DSGVO/GDPR + (nachgeordnet) BDSG neu
- EU Cybersecurity Act 2019/881 oder IT-Sicherheitsgesetzt (IT-SiG)
- EU-Richtlinie 2016/943 – Schutz von Geschäftsgeheimnissen
- BGB und HGB und darauf basierende Regelwerke (GOBD, AO)
- Strafrecht (§ 202a StGB "Ausspähen von Daten", § 303b StGB "Computersabotage")
- MaRisk oder die Anforderungen an die IT der BaFin (BAIT, VAIT)

Nota bene: JEDER IT-Job ist mittlerweile ein Security- und Compliance-Job – und der weltweite Fachkräftemangel sowie eine lebendige Gesetzeslage erleichtern diese Situation nicht gerade. Es braucht Softwaresysteme, die Unternehmen bei der Abwicklung der IAM-Prozesse unterstützen. Denn eines ist sicher: Ohne die Einhaltung von Compliance- und Sicherheitsstandards bleibt jede DT unvollendet oder endet im schlimmsten Fall in existenzbedrohenden Strafen.

2 Siehe Google Authenticator oder https://tools.ietf.org/html/rfc6238

## WEITERE ANFORDERUNGEN AN EIN IAM-SYSTEM

Die Zentralisierung der Verantwortlichkeiten in einem IAM-System bringt verschiedene nicht funktionale Aspekte ins Spiel. Ist z. B. ein Dienst auf der Digitalisierungslandkarte für den 24/7-Betrieb konzipiert, so ist das gleiche Service Level Agreement (SLA) für die IAM-Komponente erforderlich. Nur so kann jederzeit (ca. 99,8 %) ein Login in alle angebundenen Services ermöglicht werden.

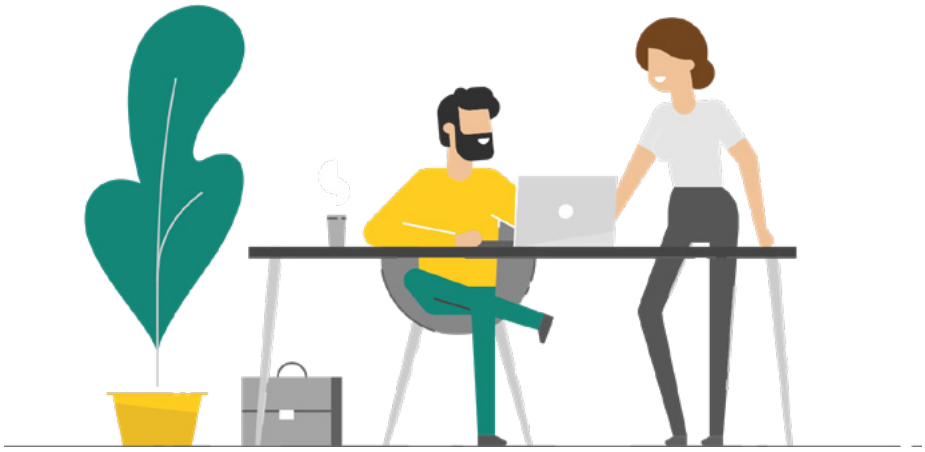
Jeder Request, auch zwischen Services, sollte authentifiziert und autorisiert werden. Doch ist die auf das IAM eingehende Request-Menge nicht zu vernachlässigen. Autorisierte Anwendungen können zudem Programmierfehler aufweisen und unnötig viele Requests in Richtung des IAM-Systems auslösen. Vorbeugende Maßnahmen können eine horizontale Skalierung, anwendungsbasierte Request-Limits sowie eine Zero-Downtime-Strategie sein, um z. B. den 24/7-Betrieb zu gewährleisten.

Authentifizierungs-Verfahren unterstützen den Einsatz von signierten JSON-Web-Tokens. Die Gültigkeitsprüfung eines digitalen Ausweises ist also auch ohne eine erneute Anfrage an das IAM-System möglich, zumindest für eine begrenzte Zeit. Ebenfalls kann die IAM-Lösung aus mehr als einem Service bestehen: So kann es praktikabel sein, den Protokollanteil (Login, Endpunkte für die Fachanwendungen) von dem Verwaltungsanteil (User-Lifecycle, IAM-Sachbearbeitung) zu trennen. Bei hohem Bedarf an Sicherheit kann für den Verwaltungsanteil auch weiterhin der Sicherheitszaun (s. o.) eingesetzt werden.

Ist die IT-Landschaft sehr heterogen – etwa durch ältere anzubindende Systeme – müssen die Identitätsinformationen in andere Anwendungen hinein provisioniert werden können. Bei der Auswahl einer IAM-Lösung sind demnach wichtig: die Kompatibilität mit den Bestandssystemen sowie zusätzliche Integrationsaufwände. Alle Anwendungen oder Services müssen die Durchsetzung der im IAM-System vergebenen Rechte unterstützen – das erfordert tiefergehendes Know-how über die jeweils anzubindenden Softwarelösungen.

Für zeitgemäße Anwendungen hat sich die attributbasierte Zugriffskontrolle (ABAC) durchgesetzt, die mit OpenID/OAuth2 konform ist. Hierbei werden den Rollen (s. o.) verschiedene technische Label in Form von Attributen zugeordnet, die anschließend zur Durchsetzung der Rechte in der jeweiligen Anwendung ausgewertet werden. Die Label sollten der Spezifikation oder dem Betriebshandbuch der jeweiligen Anwendung entnommen und im IAM konfiguriert werden können.

IAM-Standardprodukte verfügen über ein vorkonfiguriertes Konnektoren-Set für andere Stand-ardlösungen, wie z. B. Salesforce, SAP, G Suite, Office 365 & AzureAD, Adobe Sign oder



die Atlassian-Tools. Sind sie selbst ein Softwarehersteller und entwickeln einen Großteil der Digitalisierungsdienste selbst? Dann kann ein individuell entwickeltes IAM auf Basis von Halbfabriken wie dem IdentityServer oder Keycloak ein praktikabler Weg sein. Das sollte gegen zusätzliche Lizenzkosten für eine IAM-Lösung abgewogen werden. Bei einem solchen Vorhaben hilft ein kompetenter Partner als Berater, denn die richtigen technischen und fachlichen Entscheidun-gen zu treffen, kann mitunter recht knifflig sein. Nicht zuletzt bietet durchaus nicht jeder Authen-tifizierungsablauf von OAuth2 das gleiche Sicherheitslevel. Und beim Onboarding von bestehe-nden Nutzerkonten in ein neues IAM-System sind verschiedene Migrationsherausforderungen zu beachten, um einen reibungslosen Übergang sicherzustellen.

## FAZIT UND HANDLUNGSEMPFEHLUNG

Im zurückliegenden Jahr konnten wir miterleben, wie sich die Digitale Transformation aufgrund der Einschränkungen im Alltag und bei sozialen Kontakten zunehmend beschleunigt hat. Die Auswahl eines geeigneten IAM-Ansatzes bleibt dennoch eine komplexe Entscheidung und will trotz Zeitdrucks wohlüberlegt sein. Häufig entsteht nach der Einführung einer IAM-Lösung erst das eigentliche Projekt durch die Anbindung der Bestandssysteme. Deshalb ist neben intensiver Planung die Wahl einer möglichst flexiblen IAM-Lösung wichtig, die sich bestmöglich an fachkontext-spezifische Bedürfnisse anpassen lässt. Ohne eine IAM-Komponente bewegen sich bei der DT hingegen schnell alle auf technisches oder auch rechtliches Glatteis. Ganz gleich, ob Unternehmen, Behörden, Verbände oder weitere Institutionen.

Eine zentrale Herangehensweise ist beim IAM nicht nur effizient, sondern durch die Aufgaben de facto gefordert. Und natürlich sollte das IAM-System so frei von Schwachstellen und so unempfindlich gegen Angriffe wie möglich konzipiert sein. Auch an dieser Stelle hilft der Security-by-Design-Ansatz mit kontinuierlichen Pentests, Sicherheits-Verifikationsstandard (OWAPS ASVS) und weiteren möglichst frühen Qualitätssicherungs-Maßnahmen.

Die SMF GmbH hat sich in den letzten Jahren eine starke Lösungskompetenz im Bereich von DT- und IAM-Projekten erarbeitet. Erfolgreich durchgeführte Projekte kommen aus dem Energiehan-del, dem Verlagswesen, im Rahmen von IoT-Plattformen als auch aus dem öffentlichen Sektor mit mehr als einer halben Millionen Nutzern und über 60 angebunden Services.

**Phillip Conrad, M.Sc.**
Segment Manager
Finance & Service

+49 231 9644-422
p.conrad@smf.de

# GLOSSAR

**DMZ:**
Eine Demilitarisierte Zone bezeichnet ein Computernetz mit sicherheitstechnisch kontrollierten und pauschal eingeschränkten Zugriffsmöglichkeiten

**DT:**
Die digitale Transformation ist ein fortlaufender Veränderungsprozess, welcher durch digitale Technologien ermöglicht wird. Diese Technologien werden in einer immer schneller werdenden Folge entwickelt und eröffnen so den Weg für wieder neue digitale Technologien. Die Sicherheit darf hierbei nicht auf der Strecke bleiben.

**IAM:**
Rollen- und Rechteverteilung (Identity and Access Management)

**Intrusion Detection:**
Angriffserkennung auf Basis von automatisierten Heuristiken, erster Schritt in der Bekämpfung von Malware

**Least Privilege:**
Kein User verfügt über mehr Zugriffsrechte, als er braucht

**On Premises:**
Software wird eigenverantwortlich auf Hardware betrieben, die von dem Hersteller/Lizenzgeber der Software unabhängig ist

**Pentests:**
Umfassender in der Regel von unabhängigen Einrichtungen durchgeführter Sicherheitstest. (Penetrationstest)

**Privacy and Consent Management:**
Organisiert die Zustimmung zur Verwendung sensibler Daten

**Privacy by Design:**
Unabhängige und Richtlinien-basierte Unterstützung bei der Einhaltung der DSGVO in der Software-Architektur

**Robotic Process Automation:**
Automation von fehleranfälligen oder zeitaufwändigen Prozessen

**Service Level Agreement:**
Vereinbarung zur Service-Qualität und Verfügbarkeit zwischen Auftraggeber und Dienstleister für wiederkehrende Dienstleistungen

**Vendor-Lock:**
Hohe Kosten erschweren dem Verbraucher/Nutzer einen Anbieterwechsel da ein System an einer Infrastrukturkomponente gebunden ist

**Zero-Downtime-Strategie:**
Architekturvorgehen zur Ermöglichung eines Rund-um-die-Uhr-Betriebs

**Security-by-Design:**
Etablierung von Architekturrichtlinien, um Sicherheitsanforderungen an Soft- und Hardware schon während der Entwicklungsphase eines Produktes zu berücksichtigen

# WO WIR SIND

SMF GmbH
Paul-Henri-Spaak-Str. 5
44263 Dortmund

T. +49 231 9644-0
F. +49 231 9644-100

smf.de/iam