Kennzahlen statt ROI!

Fachartikel von Peter Weierich, Managing Director Germany

„Projekte müssen sich innerhalb eines Jahres rechnen." Mit derartigen Postulaten können Unternehmen nur in Ausnahmefällen ein IAM-Programm starten. Denn die wenigsten Projekte amortisieren sich finanziell. Trotzdem sind Erfolge von IAM-Projekten messbar - indem man Kennzahlen verwendet.

Unterschiedliche «ROI-Fallen» lauern

Mit klassischen ROI-Überlegungen in IAM-Programme einzusteigen, lässt die Projekte in unterschiedliche Fallen laufen: Zum Ersten kann die Automatisierung zwar Administrationskosten einsparen. Nur in Ausnahmefällen, wenn bislang sehr viel manuell verwaltet wird und das Unternehmen ausreichend groß ist, ist eine Payback-Zeit nachweisbar. Es gibt allerdings einige Sonderfälle, in denen sehr schnell eine gesamtwirtschaftliche Rentabilität erzielt wird: Wenn man den „Ich habe mein Passwort vergessen" Prozess automatisiert, sind die Vergesslichen bei einer Toolunterstützung viel schneller produktiv als bei einer Helpdesk-basierten Vorgehensweise. Single Sign-On Projekte helfen den Usern wertvolle Zeit bei der Anmeldung an vielen Systemen und der Passwortverwaltung einzusparen. Schließlich kann der Produktivitätsgewinn eines IdMs beziffert werden, wenn ein neuer Mitarbeitender ab der ersten Arbeitsminute Zugriff auf die IT-Systeme hat und nicht stunden- oder sogar tagelang auf seine Zugänge warten muss. Die so „gewonnene" Arbeitszeit wird allerdings nicht den Kostenstellen der IT gutgeschrieben, welche die Kosten einer Implementierung zu tragen hat.

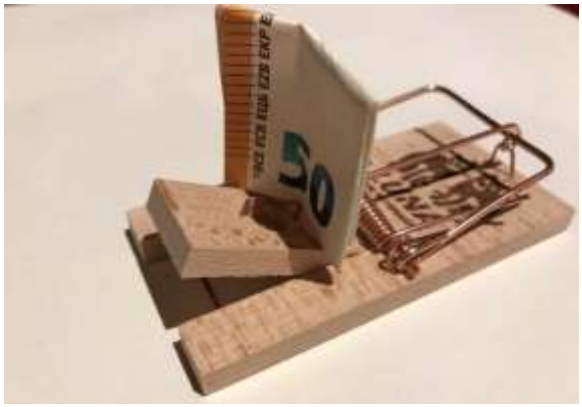

Abb. 1: Wer nur auf pekuniäre Effekte von IAM-Programmen setzt, läuft oft in eine Legitimationsfalle.

Eine dritte „Falle" lauert regelmäßig bei outgesourctem IT-Betrieb: Da die Einkäufer immer nur „billig" einkaufen wollen und Effizienzgewinne in den Vertragswerken gar nicht vorgesehen sind, hat in der Regel mindestens eine der Parteien ein Interesse an einer Automatisierung: Der Dienstleister nicht, weil das ja die Anzahl der kostenpflichtigen Tickets reduzieren würde. Bei Pauschalverträgen dagegen hat der Kunde keine Motivation neue Prozesse einzuführen, da er damit ja „nichts spart".

Dimensionen der Kennzahlen

Trotzdem lohnt es sich in jedem Fall den Nutzen von IAM-Projekten messbar zu machen. Das gilt umso mehr als vielfach Compliance-Anforderungen die eigentlichen Treiber sind. Kennzahlen können dabei nach Klassen eingeteilt werden:

- Effizienz misst im Wesentlichen den Automatisierungsgrad
- Effektivität adressiert vor allem compliance-getriebene Anforderungen
- Enablement misst die Nutzeneffekte außerhalb der IT, also beispielsweise Auswirkungen auf die Geschäftsentwicklung

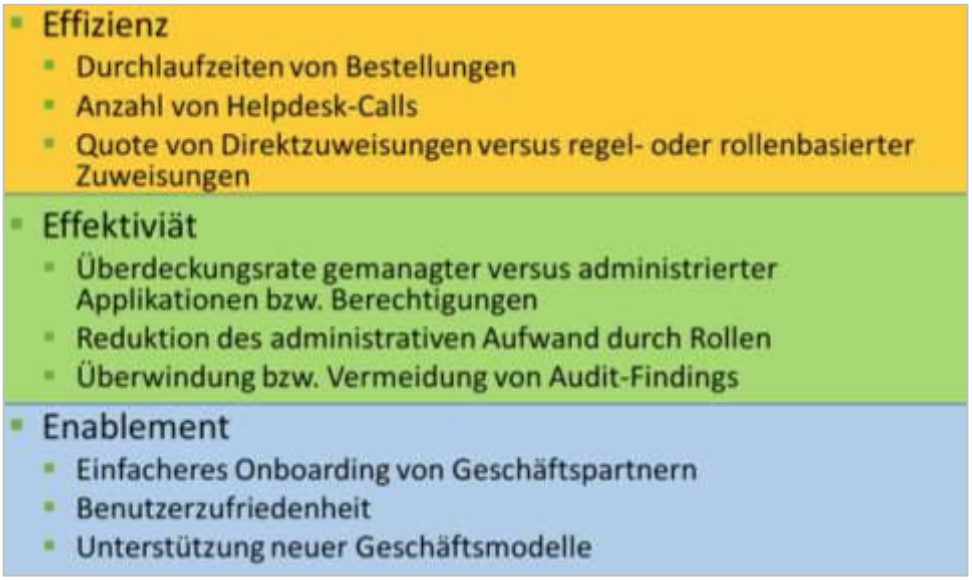

Abb. 2: Klassifizierung Kennzahlen IAM-Projekt

Der Klassiker: Passwort vergessen

Der Passwort-Reset ist der Klassiker unter den Automatisierungsprojekten: Je nach Kalkulation kostet ein „vergessenes“ Passwort oder ein zu spät neu gesetztes Passwort betriebswirtschaftlich zwischen 20 und wenigen hundert Euro. Mit Toolunterstützung kann man den Service-Desk wirksam entlasten: Derzeit arbeiten die meisten Tools mit der Abfrage von privatem Wissen, zum Beispiel der ersten Automarke oder dem Mädchennamen der Mutter. Verfahren der Nachbarschaftshilfe stellen beispielsweise zwei Kollegen jeweils eine Hälfte des neuen Passworts zu. Besser geschützt gegen social Engineering Angriffe ist man dagegen durch biometrische Verfahren: Seit über einem Jahrzehnt haben Unternehmen Stimmerkennung zur Authentisierung im Einsatz. Andere Verfahren sind prinzipiell verfügbar, allerdings muss in einer Gesamtkostenkalkulation auch der Aufwand für das Enrollment, also beispielsweise das Erfassen von Stimm-Mustern eingerechnet werden.

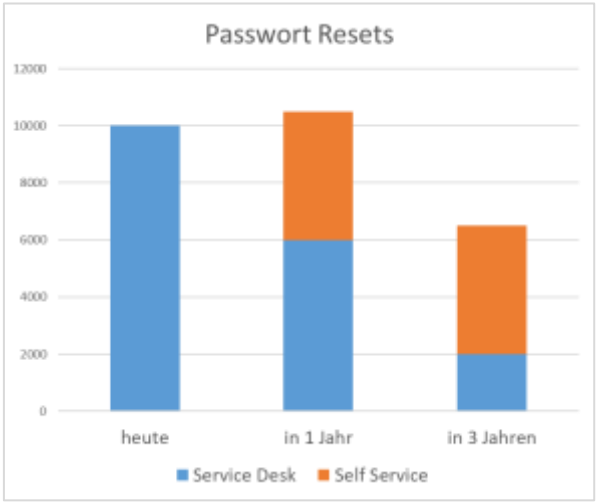

Abb. 3: Toolunterstützung entlastet Service-Desk markant

Ein weiteres Mittel, die Anzahl von Passwort Resets insgesamt zu reduzieren, sind SSO-Methoden. Das wird durch die Integration von möglichst vielen Anwendungen in die zentrale Anmeldung (meist via Active Directory) oder die Einführung von dezidierten Single Sign-On Produkten bzw. Federation-Technologien erreicht: Dann müssen sich Anwender nämlich insgesamt weniger Benutzernamen-Passwort-Kombinationen merken.

Effekte von Single Sign-On

Gut mit Kennzahlen belegen lässt sich die Anzahl von Anwendungen, an denen sich ein User explizit „anmelden“ muss. Viele Silosysteme sind nämlich nicht nur aus Mitarbeitersicht ineffizient. Sie stellen zusätzlich ein erhebliches Sicherheitsrisiko dar: Wenn Passwörter auf Post-its geschrieben oder unter der Schreibtischablage zu finden sind, könnte man auch gänzlich auf sie verzichten. Oft ist es der einfachste und kostengünstigste Weg, Applikationen in das führende Directory zu integrieren. Klassische SSO-Produkte kommen zwar generell immer mehr „aus der Mode“, weil die Directory-Integration immer weiter fortschreitet. Sie erleben jedoch vor allem in Krankenhäusern derzeit eine Renaissance, weil sie auch einen schnellen Benutzer- bzw. Sessionwechsel auf den Stationsrechnern erlauben.

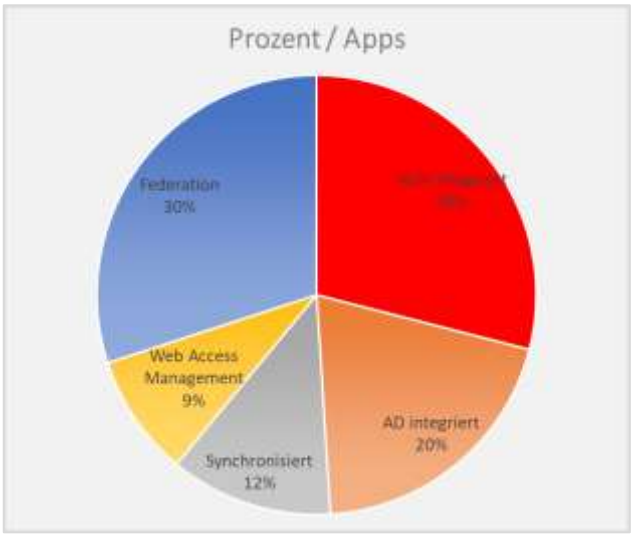

Abb. 4: Kennzahlen App-Nutzung

Ohnehin schwindet die Relevanz klassischer thick clients: Neu eingeführte Anwendungen sind meistens webbasiert – unabhängig davon ob sie intern betrieben werden oder von einem externen Cloud-Anbieter. Dafür werden die früher implementierten Web-SSO-Lösungen zunehmend abgelöst durch Standard-basierende Federationtechnologien. Diese haben zusätzlich den Vorteil, dass sie bei Bedarf eine on-the-flight Provisionierung ermöglichen, also eine Neuanlage von Accounts auf der Grundlage einer Vertrauensstellung.

Allerdings kann die Zählung der Integrationsart von Applikationen ein verzerrtes Bild der gelebten Wirklichkeit abgeben: Wenn es viele Anwendungen gibt, die sehr wenige User haben, die diese auch noch selten nutzen, kann die Statistik unangemessen negativ aussehen. Ideal wäre es, die realen Zugriffe zu zählen. Wenn diese Information nicht verfügbar ist, gibt immerhin eine Statistik über alle Accounts in den einzelnen Applikationen ein gutes Bild.

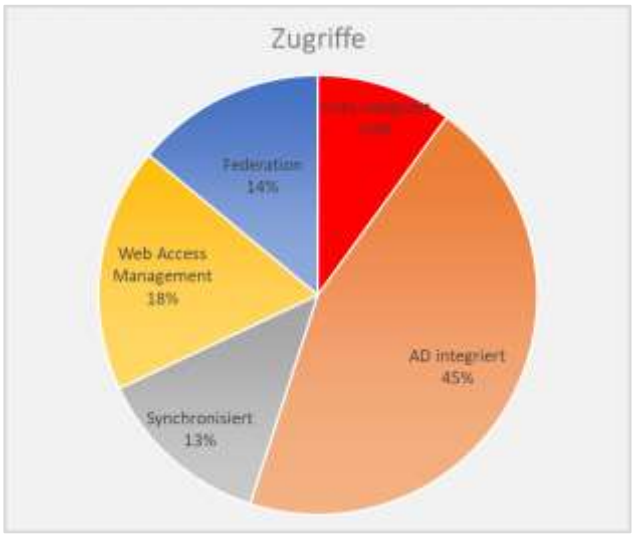

Abb. 5: Kennzahlen App-Zugriffe

Privilegierte Accounts

Derzeit wächst in vielen Unternehmen das Bewusstsein, dass privilegierte Accounts ein Sicherheitsrisiko darstellen. Nicht nur in regulierten Branchen erkennt man, dass Administratoren-Accounts, die von mehreren Personen genutzt werden nicht mehr existieren dürfen: Jeder Administrator muss zukünftig mit personalisierten Accounts arbeiten. Oft werden dezidierte Privileged Account/Access Management (PAM) Produkte eingeführt, die den privilegierten Usern eigene Sessions bereitstellen und sie damit sogar davon entlasten, sich komplexe Admin-Passwörter zu merken. Allerdings ist es auch möglich, das Management der Accounts selbst im IdM abzubilden.

In jedem Fall ist es sinnvoll, Kennzahlen für eine initiale Bestandsaufnahme sowie für die Formulierung von kurz- und langfristigen Zielen zu erheben. Für die folgenden Accountarten sollten die Anzahl erhoben werden und der Anteil gemanagter Accounts – unabhängig davon, ob das mit einem PAM-Produkt oder dem IdM-System erfolgt:

- **Admin-Accounts:** Hier unterstellen wir, dass diese Accounts bereits auf personengebundene Accounts „umgestellt“ wurden. Sonst müsste auch gezählt werden, wie viele Personen mit geteilten Admin-Accounts arbeiten.
- **System Accounts:** Bei diesen Accounts, die meistens von Applikationen verwendet werden, muss mindestens ein Verantwortlicher hinterlegt sein. Das kann eine Person oder auch eine Rolle sein. Dabei muss sichergestellt sein, dass beim Ausscheiden einer verantwortlichen Person immer ein Nachfolger bzw. Stellvertreter bekannt ist.
- **Emergency oder Firefighter Accounts**: Diese werden prinzipiell nur zeitlich befristet vergeben, um akute Probleme zu lösen.
- **Externe Accounts:** Hierbei handelt es sich um privilegierte Zugänge von externen Partnern, also von IT-Dienstleistern oder auch Produktherstellern, die im Supportfall auf Systeme zugreifen müssen.

Für jeden dieser Account-Typen können in einer Roadmap kurz- und mittelfristige Ziele vorgegeben werden, die geprägt werden von den Sicherheitsanforderungen sowie dem Aufwand. Der rein technische Aufwand ist dabei oft vergleichsweise klein. Häufig verzögern historisch gewachsene und schlecht dokumentierte Strukturen bei den Systemaccounts ein durchgängiges «Management» und muss durch einen organisatorischen Prozess begleitet werden.

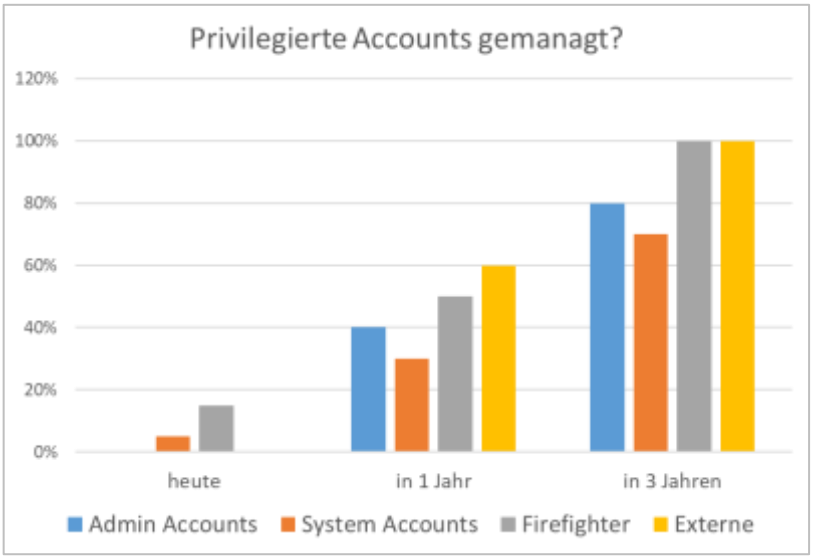

Abb. 6: Der Reifegrad des Managements privilegierter Zugriffe kann für jeden Accounttyp gesondert geplant werden.

Businessrollen machen Sinn – aber nicht zu viele davon!

Immer mehr Unternehmen führen Geschäftsrollen ein, die möglichst viele Einzelberechtigungen aus unterschiedlichen Applikationen beinhalten. Das fördert die Transparenz und reduziert den Verwaltungsaufwand. In stark regulierten Branchen, beispielsweise Banken, erzwingen mittlerweile die Aufsichtsbehörden die Einführung von Geschäftsrollen. Ein gängiges Missverständnis dabei ist: In keinem Fall wird gefordert, dass ausnahmslos alle Berechtigungen über Geschäftsrollen vergeben werden: Diese Forderung würde nämlich zu einer «Explosion» der Anzahl von Geschäftsrollen führen und die Transparenz sogar verschlechtern anstatt zu verbessern.

Ohne an dieser Stelle auf Details der Einführung von Geschäftsrollen einzugehen, unterscheiden wir die folgenden Zuweisungswege über die Benutzer Berechtigungen erhalten (haben):

1. Direktzuweisung ohne klare Prozesse, das heißt Zuweisung auf «Zuruf» oder über Freitextbestellungen, die dann ohne festgelegte Regeln von einem Adminteam o.ä. umgesetzt werden. Dieser Zuweisungsweg ist bei Weitem der Schlechteste, spiegelt in vielen Organisationen allerdings den aktuellen Status Quo wider.
2. Einzelzuweisungen über einen klar geregelten Antragsprozess: Berechtigungen werden beantragt, bei Bedarf genehmigt und dann manuell oder automatisch zugewiesen.
3. Geschäftsrollen: Möglichst viele Einzelberechtigungen werden durch Geschäftsrollen gebündelt und dann entweder über Regeln zugewiesen oder über Anträge bzw. Bestellungen. Die Regeln können sich auf Organisationszugehörigkeiten, Standorten, Funktionen etc. beziehen. Grundsätzlich empfehlen wir Geschäftsrollen über beide Wege zuweisbar zu machen.
4. Regeln / Policies: Dabei werden Berechtigungen direkt in Abhängigkeit von Organisationszugehörigketen o.ä. vergeben. Beispielsweise kann die automatische Zuweisung von Abteilungslaufwerken über Regeln erfolgen.

Ein optimaler Zielzustand ist derjenige, der möglichst viele Berechtigungen über Regeln und Geschäftsrollen zuweist und gleichzeitig die Anzahl dieser Regeln und Geschäftsrollen nicht zu sehr wachsen lässt.

Die Abbildung 7 zeigt daher einen möglichen Fahrplan der Reifung von Berechtigungszuweisungen: Initial sind bereits einige Regeln umgesetzt, ansonsten ist allerdings nicht nachvollziehbar, wer warum und wann welche Berechtigung erhalten hat. In einer Pilotphase wird ein Teil der Berechtigungen über ein strukturiertes Verfahren «bestellbar» gemacht. In Phase 3 erfolgt der Ausbau des Bestellsystems und gleichzeitig die Pilotierung von Geschäftsrollen. Im Zuge der Reifung der Prozesse wird sowohl das Rollenmanagement sowie das Regelwerk ausgebaut und idealerweise alle anderen Berechtigungen über einen gut dokumentierten Antragsprozess geführt.

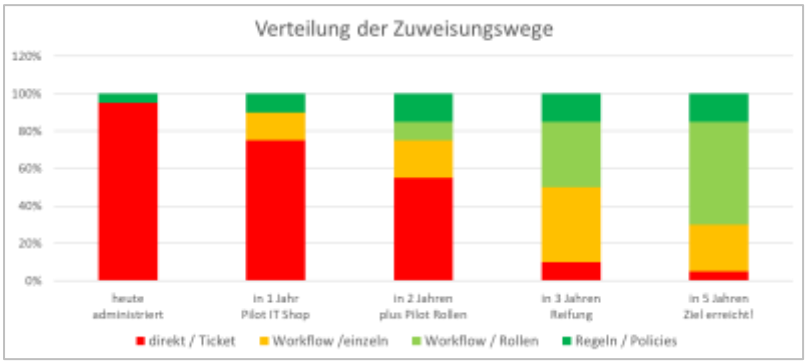

Abb. 7: Der Reifegrad des Managements privilegierter Zugriffe kann für jeden Accounttyp gesondert geplant werden.

C-IAM ist mit Marketing-Sprech

Beim Customer-IAM (C-IAM) Programmen prägen vor allem Marketing-Kennzahlen und das entspechende Wording die Denkweise. Das gilt am stärksten für C-IAM Projekte, bei denen das «C» für «Consumer» steht, also für idealerweise viele Millionen (potenzieller) Endkunden.

Daher sind typische Kennzahlen beispielsweise:

1. Enrollment
    - Anzahl von Neu-Registrierungen
    - Befüllungsgrad von Profilen
    - Newsletter-Abos
    - Registrierungen über Federation (z.B. Google, Facebook oder Amazon) bzw. Affiliate Marketing
    - Empfehlungen durch andere Mitglieder / Kunden
    - Erfolgsmessung von Kampagnen
2. Wiederkehrer
    - Anzahl von Social-Logins, abhängig vom Identity Provider
    - Quote von Re-Visits
    - Anzahl von Re-Visits
    - Käufe bzw. Geschäftsabschlüsse
    - Erfolgsmessung von Kampagnen
3. Cross-Selling
    - Positionieren weiterer Produkte
    - Nutzung anderer Portale eines Konzerns (z.B. bei Adidas oder Bayer)
    - Erfolgsmessung von Kampagnen
4. Nicht-Nutzung bzw. Probleme
    - Abbrüche von Registrierungen z.B. wegen fehlender Rückbestätigungen (DOI: Double opt-in)
    - Abbrüche während der Bestellprozesse
    - Inaktivität, erzwungene Löschungen aufgrund zu langer Inaktivität, Erfolgsquote von Re-Aktivierungen
    - Passwort-Resets (erfolgreiche und nicht erfolgreiche)

Bei komplexen C-IAM-Szenarien mit vielen Services sind oft der Aufwand für die Integration sowie die absolute Anzahl von Services wichtige Kennzahlen.

Im C-IAM-Umfeld gibt es zudem immer häufiger Benchmarks, die über viele Kundenportale hinweg Kennzahlen erheben. Neben Usability-Messungen [Weierich et al. 2016] kann die Compliance von Kundenportalen

bezüglich der Umsetzung der GDPR-Regeln ausgewertet werden. In [iWelcome 2018] wurden 139 Kundenportale aus acht Ländern (EU & USA) und sechs verschiedenen Branchen untersucht. Die folgenden Kriterien wurden evaluiert:

- Zustimmung (consent) zur Speicherung und Verarbeitung der Daten
- Möglichkeit, die Zustimmung zurückzuziehen (ability to withdraw)
- Einsichtnahme in die gespeicherten Daten (right of access)
- Möglichkeit, fehlerhafte Daten zu korrigieren (right of rectification)
- Recht zur Löschung der Daten (right to erasure)
- Speicherzeit (data retention period): Transparenz der Speicherdauer
- Privatsphäre als Standard (privacy as default): Beispielsweise darf das «Newsletter-Abo» nicht standardmäßig aktiviert sein.
- Sensitive Daten (special categories of data): Werden sensitive persönliche Daten z.B. bezüglich der Herkunft, der sexuellen, politischen oder religiösen Präferenzen besonders geschützt?

Erwartungskonform schnitten die USA dabei besonders schlecht ab; Deutschland, Schweden und UK sehr gut und die Niederlande, Schweiz, Spanien und Frankreich hatten noch deutliches Verbesserungspotenzial.

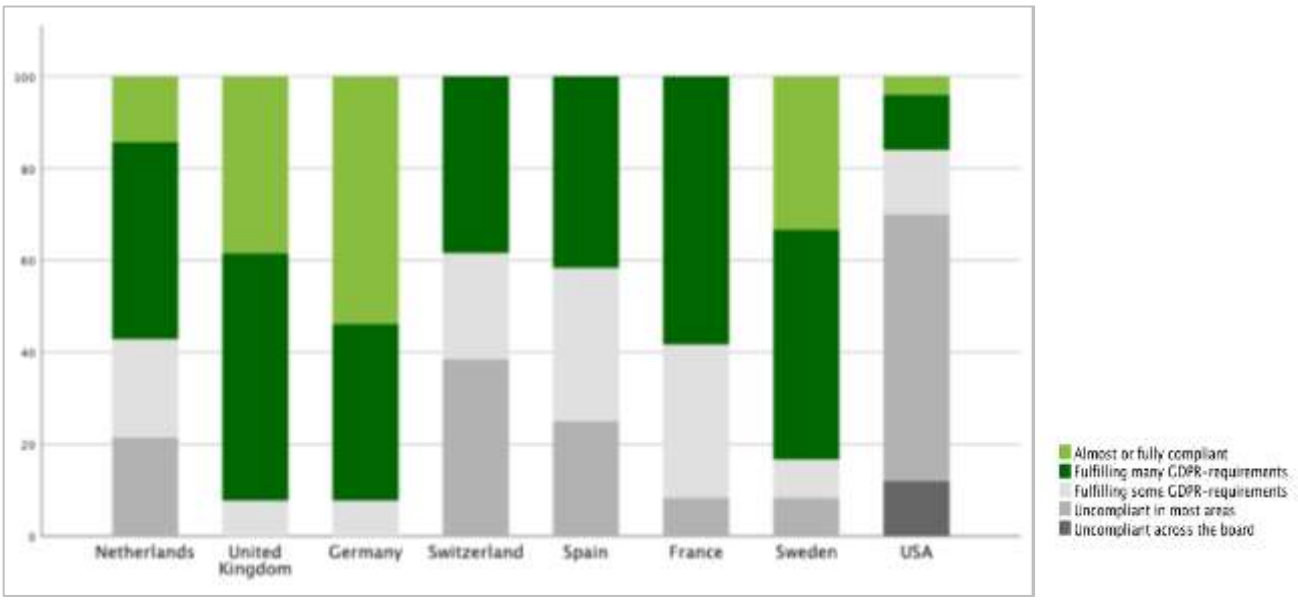

Abb. 8: Die Umsetzung von GDPR-Regeln wurde von [iWelcome 2018] für mehr als 200 Kundenportale evaluiert.

Fazit

Erfolge von IAM-Projekten amortisieren sich nur sehr selten durch Einsparungen. Bevor man in eine der «ROI-Fallen» tappt, lohnt es sich, die Kennzahlen zu erheben und idealerweise über Jahre zu beobachten. Aus den Dimensionen Effizienz, Effektivität und Enablement können der Reifegrad und auch die Umsetzung von Compliance-Vorgaben messbar gemacht werden.

Wie unterstützt IPG?

Als Experte für IAM unterstützen wir Sie gerne in der strategischen Planung, der Umsetzung und dem Betrieb von effektiven und effizienten Lösungen rund um die Verwaltung von Identitäten und Zugriffen. Unsere Advisory Services zeigen Ihnen auf, wie Sie die Kennzahlen ermitteln und für Ihre Planung einsetzen können.

Kontaktieren Sie uns, wenn Sie mehr zu diesem Thema erfahren möchten.

Christian Rückert: Sales Manager Germany
christian.rueckert@ipg-group.com; Telefon +49 170 908 03 53

Markus Blaha: Sales Manager Austria an Switzerland
markus.blaha@ipg-group.com; Telefon +43 (676) 734 23 00

Literatur / Quellen:

[Weierich et al. 2016] Peter Weierich, Tobias Schmidt und Sebastian Abeck; Usability der Identity- und Accessmanagementkomponenten von Endkundenportalen; in INFORMATIK 2016, Lecture Notes in informatics (LNI), Gesellschaft für Informatik, 2016

[iWelcome 2018] The state of GDPR-readiness in Europe 3rd edition April 2018, https://www.iwelcome.com/the-state-of-gdpr-readiness-in-europe-report-v3