Blog Post

N° 4/2018

Erfolgsfaktoren für e-Identity-Systeme

Empfehlungen für eine akzeptierte, kompetitive und fortdauernde e-Identity-Lösung

Dr. Andreas Windisch

ASQUARED

asquared Blog Post N° 4/2018

März 2018

Digitale Identitäten sind in aller Munde und europaweit existiert aktuell eine Vielzahl unterschiedlicher Ansätze. Auf Basis von Kim Cameron's Laws of Identity stellen wir neun Erfolgsfaktoren für e-Identity-Systeme vor. Diese zu beachten, wird der Schlüssel zur Etablierung einer akzeptierten, kompetitiven und fortdauernden Lösung sein: Neben der Akzeptanz auf Service Provider- und Kundenseite geht es insb. um die Erschließung innovativer Geschäftsfelder zur Schaffung von Mehrwert.

Einleitung

US-amerikanische Anbieter sind seit Jahren als Identitäts-Provider etabliert (z. B. Facebook, Google, LinkedIn). Die Accounts können bereits genutzt werden, um sich komfortabel auf diversen Seiten einloggen zu können, ohne sich immer neu registrieren zu müssen. Sie fokussieren bislang aber auf „einfache Identitäten". Asiatische Unternehmen wie Tencent haben in ihren Heimatmärkten vor allem mit WeChat eine beachtliche Reichweite erreicht und sind dabei, die Accounts zu anerkannten elektronischen Identitäten zu erweitern und die Funktionalität weltweit auszurollen; Deutschland wurde dabei als erstes besonders interessantes Internationalisierungsziel ausgewählt.

Als Reaktion darauf und nicht zuletzt wegen der sich ändernden regulatorischen Anforderungen an den Datenschutz - im Wesentlichen die europäische Datenschutz-Grundverordnung sowie die neue e-Privacy-Richtlinie - sind digitale Identitäten und etwaige e-Identity-Systeme (Infrastrukturen, Plattformen und/oder Schemes) in aller Munde. In Europa sprießen e-Identity-Systeme aus dem Boden: Von staatlichen Lösungen als Digitalisierungsbestreben der bestehenden Identifizierungsmittel über kleinere Startups, Lösungen auf Basis innovativer Technologie oder Lösungen einzelner Branchen bis hin zu branchenübergreifenden Kooperationsansätzen. In einigen europäischen Ländern findet dieser Prozess bereits seit vielen Jahren sehr differenziert statt, in Deutschland rückt es sich noch zurecht. Unser Blogbeitrag „E-Identity-Lösungen in Europa" gibt einen zusammenfassenden europaweiten Überblick.

Spannend bleibt, welches der Systeme sich mit Blick auf die Marktakzeptanz durchsetzen kann. Zur Einschätzung dieser Frage können Kim Cameron's Laws of Identity zu Rate gezogen werden. Kim Cameron hat bereits im Jahr 2005 eine Liste von Gesetzmäßigkeiten für digitale Identitäten zusammengefasst, die den Erfolg oder den Misserfolg digitaler Identitätssysteme erklären. Diese Gesetzmäßigkeiten haben wir auf die aktuellen Gegebenheiten im Jahr 2018 angewandt, bewertet, ob diese weiterhin Gültigkeit haben und darauf aufbauend eine Liste von Erfolgsfaktoren für moderne e-Identity-Systeme abgeleitet, die es für e-Identity-Anbieter gilt zu beachten.

The Laws of Identity von Kim Cameron

Kim Cameron ist Identity Architect bei Microsoft und hatte eine führende Rolle in der Entwicklung einer Vielzahl Identity-relevanter Microsoft Produkte. Vor vielen Jahren bereits widmete er sich der Herausforderung, dass das Internet ohne expliziter Möglichkeit entwickelt worden ist, zu wissen, mit wem man interagiert, weshalb sich die digitalen Service Provider seit jeher diverser Workarounds bedienen.

> *„[…] Today's Internet, absent a native identity layer, is based on a patchwork of identity one-offs."*
>
> *Kim Cameron, Microsoft Corporation, 2005*

In *The Laws of Identity* verdeutlichte er im Jahr 2005 die Relevanz eines übergreifenden Identity Layers, erläuterte gleichzeitig jedoch die Herausforderungen bei der Etablierung eines solchen Layers. Cameron war sich bereits damals sicher, dass eine „einzige simplifizierte digitale Identitätslösung als universelles Allheilmittel nicht realistisch" sei.

Stattdessen werde zur Adressierung digitaler Identitäten ein vereinheitlichendes Identitäts-Metasystem benötigt, welches gemeinsame Standards definiert und unterschiedliche Identitätslösungen aus unterschiedlichen Anwendungskontexten lose koppelt.

Zur Definition eines solchen Identity Layers hat Cameron federführend 7 Gesetzmäßigkeiten für digitale Identitäten (7 Laws of Identity) zusammengefasst und empfiehlt, diese strikt zu befolgen, um so ein Identitäts-Metasystem zu erzeugen, welches allgemein und fortdauernd Akzeptanz erfährt.

Erfolgsfaktoren für e-Identity-Systeme

Die Anwendbarkeit und Relevanz von Cameron's Laws of Identity haben wir gegeben unserer Erfahrung auf dem Gebiet digitaler Identitäten und unseren Einschätzungen zu den aktuellen Marktgegebenheiten analysiert und auf dieser Basis insgesamt neun Erfolgsfaktoren für e-Identity-Systeme abgeleitet.

Im Vergleich zu den Empfehlungen von Cameron haben wir einen Punkt etwas erweitert (Erfolgsfaktor 6) sowie zwei aus unserer Sicht erfolgskritische Punkte separat herausgestellt (Erfolgsfaktoren 8 und 9). Die restlichen Punkte haben u. E. weiterhin unverändert Gültigkeit. Die nachfolgende Grafik fasst die Erfolgsfaktoren kondensiert zusammen, die darauffolgenden Absätze erläutern diese etwas ausführlicher und bewerten sie vor dem Hintergrund des Status Quo der gegebenen Marktsituation.

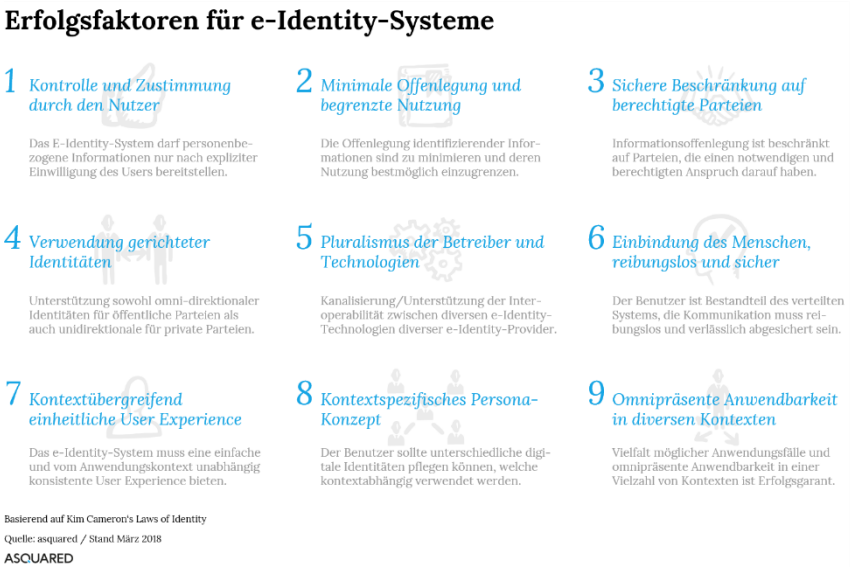

Abbildung 1: *Neun Erfolgsfaktoren für e-Identity-Systeme / Stand März 2018*

Erfolgsfaktor 1 - Kontrolle und Zustimmung durch den Nutzer

Der Erfolg eines e-Identity-Systems hängt maßgebend vom Vertrauen des Benutzers ab. Vertrauen wird an dieser Stelle geschaffen durch die übergreifende Verpflichtung des Identity-Systems, den Benutzer als ultimativ beherrschende Entscheidungsinstanz über die Preisgabe seiner Informationen zu setzen. So erwarten die User selbstbestimmt darüber zu entscheiden, welche Informationen über sie warum an wen übermittelt werden. Man kennt derartige Freigaben aus den App-Stores von z. B. Apple und Google, bei denen man für jede herunterzuladende App bestätigt, welche Daten und Funktionalitäten freigegeben werden. Zusätzlich bietet es sich an, dem Benutzer einen „Freigabe Manager" zur Verfügung zu stellen, der die in der Vergangenheit erteilten Freigaben aufführt und diese auch für zukünftige Anfragen wiederrufen lässt.

Allein die neue Datenschutzgrundverordnung sowie die e-Privacy-Richtlinie erfordern eben diese Grundsätze, wenngleich auch nicht in vollem Umfang. Für die e-Identity-Systeme gilt dabei also durch weitere, d.h. über die reine fallbezogene Freigabe von Informationsoffenlegungen hinausgehende Funktionalitäten, dem Benutzer die Kontrolle über seine Daten zu geben und somit das Vertrauen in das e-Identity-System zu erhöhen und – wichtiger noch - zu bewahren.

Diese Notwendigkeit haben mittlerweile (fast) alle etablierten Player verinnerlicht. Google und Facebook beispielsweise versuchen bereits seit vielen Monaten, das Thema Datenschutz und Privatsphäre sowie die Selbstbestimmtheit der Nutzer bezüglich ihrer Daten medial in den Vordergrund zu stellen. Beide haben im Jahr 2017 bzw. 2018 unterschiedliche Transparenz-Offensiven gestartet, um die Benutzer darüber aufzuklären,

bieten mittlerweile diverse Konfigurationsmöglichkeiten an und wollen diese weiter ausbauen. In China scheint man da noch nicht so weit zu sein: Es laufen bereits erste Piloten, den Messaging Dienst WeChat als elektronisches ID-Verfahren zu nutzen; Datenschutz und Privatsphäre erscheinen ungeklärt. Interessant vor allem dann, wenn der Dienst nach Deutschland kommt.

Erfolgsfaktor 2 - Minimale Offenlegung und begrenzte Nutzung

Beim Umgang mit personenbezogenen bzw. identifizierenden Informationen sind stets die „need to know"- und „need to retain"-Prinzipien anzuwenden. Deren Einhaltung ist bereits in den BSI IT-Grundschutz-Katalogen gefordert und spätestens durch die Datenschutzgrundverordnung Pflicht.

Für e-Identity-Systeme haben diese Prinzipien jedoch einen besonders hohen Stellenwert, da sie auch für die Offenlegung von Daten gegenüber Service Providern gelten und einzuhalten sind. Cameron nannte das Beispiel der Altersverifikation, bei der lediglich eine Bestätigung der Zugehörigkeit zu einer Altersklasse übermittelt werden soll, anstelle des konkreten Geburtsdatums oder auch die Vermeidung konkreter eineindeutiger Identifier, die kontextübergreifend nutzbar sind.

> *„Aggregation of identifying information also aggregates risks. To minimize risk, minimize aggregation."*
>
> *Kim Cameron, Microsoft Corporation, 2005*

Grundsätzlich dürfen die Daten nur anwendungsfallbezogen und zweckgebunden bereitgestellt werden. Je Anwendungsfall sind stets die am geringstmöglich identifizierenden Daten weiterzugeben, um die Privatsphäre des Benutzers maximal zu schützen.

Erfolgsfaktor 3 - Verlässliche Beschränkung auf berechtigte Parteien

Das e-Identity-System muss sicherstellen, dass alle beteiligten Parteien einen notwendigen und berechtigten Anspruch haben, Teil der Identitäts-Wertschöpfungskette zu sein. Dabei kann es sich um den Identity-Provider handeln, der personenbezogene Daten an das e-Identity-System bereitstellt oder aber auch um den Service Provider, der diese Daten empfängt. Der Benutzer muss sich stets darauf verlassen können, sowohl dass es sich bei diesen Parteien um die tatsächlichen Parteien handelt als auch dass lediglich die freigegebenen Daten bereitgestellt werden und diese Daten für den freigegebenen Zweck verwendet werden.

Ersteres ist heutzutage durch Verwendung von PKI-Infrastrukturen und Zertifikaten kein größeres Problem mehr. Letzteres lässt sich durch explizite Vereinbarungen bzgl.

der Datenübergabe und -verwendung zwischen den Parteien lösen. Im Einklang mit Erfolgsfaktor 1 ließen sich die gewährten Benutzungsrechte einzelner Daten je konkreter Transaktion im „Freigabe Manager“ protokollieren.

Das e-Identity-System erhält dabei gewisse Know-Your-Customer-Pflichten, um Zuwiderhandlungen einzelner Parteien innerhalb des Systems direkt zu ahnden und dadurch das Risiko für alle weiteren Parteien zu reduzieren.

Erfolgsfaktor 4 – Verwendung gerichteter Identitäten

Das Konzept gerichteter Identitäten unterscheidet die Sichtbarkeit und Kommunikationsrichtung der Identitätsentitäten. Bei omnidirektionalen Identitäten handelt es sich um solche, die öffentlich bekannt und sichtbar bzw. zugänglich sind und zu einer Kommunikation einladen: Es kann sich um einen Beacon in einem physischen Geschäft handeln, ein Kartenlesegerät oder aber auch Online um einen Webshop.

Während diese Omnidirektionalität der Identität für öffentliche Parteien sinnvoll ist, muss sie für private Identitäten strikt vermieden werden. Eine Kommunikation darf nur mit zuverlässigen und vertrauenswürdigen Parteien initiiert werden, im Idealfall nach Zustimmung des Benutzers (unidirektionale Identität). Streng genommen sind NFC- oder RFID-fähige Zahlkarten und ältere Ausweise Negativbeispiele, da darüber identifizierende Informationen (Kontodaten bzw. Personendaten) ausgelesen werden können, ohne dass eine Prüfung der auslesenden Instanz oder eine explizite Zustimmung des Benutzers stattfindet.

Insbesondere bei höherwertigen Identifikations-Use Cases sollten ausschließlich unidirektionale Identitäten für private Parteien im Einklang mit Erfolgsfaktor 1, d.h. unter Kontrolle und nach Zustimmung des Nutzers, ermöglicht werden.

Erfolgsfaktor 5 - Pluralismus der Betreiber und Technologien

Ein e-Identity-System ist nur so viel Wert, wie der Kontext in dem es Anwendung findet. Die Vielzahl dieser Kontexte und deren spezifische Charakteristika erschweren die Vereinheitlichung in einem übergreifenden System und dessen Akzeptanz auf Benutzerseite. Cameron ist noch deutlicher:

> *„One reason there will never be a single, centralized monolithic system is because the characteristics that would make any system ideal in one context will disqualify it in another.“*
>
> *Kim Cameron, Microsoft Corporation, 2005*

Ein e-Identity-System muss laut Cameron polyzentrisch und polymorph sein, d.h. es muss ein Zusammenschluss mehrerer spezifischer e-Identity-Systeme sein und daher kontextabhängig in unterschiedlicher Form existieren; ein Metasystem als System aus Systemen.

An dieser Stelle muss jedoch konzeptuell unterschieden werden, ob die Gesamtheit der identifizierenden Informationen zentralisiert in einem monolithischen System vorliegen oder lediglich die Authentifizierungsinformationen (Logins) und ggf. elementare identifizierende Informationen. Cameron spielt insbesondere auf den ersten Fall an. Im zweiten Fall werden lediglich die Benutzerauthentifizierung vereinheitlicht und identifizierende Informationen, die in fast allen Kontexten Relevanz haben, in einem monolithischen System vorgehalten, während für darüber hinaus gehende Informationen und Features ggf. ebenso polyzentrisch auf spezifische e-Identity-Systeme zurückgegriffen werden kann. In diesem Fall sollten Vorkehrungen getroffen werden, um die Akzeptanz des Systems für kontextübergreifende Anwendungsfälle sicherzustellen, vgl. Erfolgsfaktor 8 „Unterstützung kontextabhängiger Personas".

Bei den etablierten Playern wie beispielsweise Google, Facebook oder LinkedIn handelt es sich demgegenüber um monolithische Systeme, die die personenbezogenen Daten jeweils in einem Zentralsystem (auch wenn dieses technisch mit einer Vielzahl von Systemen realisiert ist) verarbeiten und vorhalten. Dies funktioniert wunderbar für elementare und nicht verifizierte Identitätsdaten. Sobald es darüber hinaus geht, werden die Schwächen dieses Ansatzes deutlich. Verifizierte Informationen beispielsweise oder kontextspezifische Attribute müssten jeweils ins Zentralsystem integriert werden und die Benutzer müssten stets bereit sein, alle Daten an eben dieser einen Stelle (Facebook? Google?) zu pflegen. Bei nicht allen Kontexten wird diese Bereitschaft vorhanden sein.

Erfolgsfaktor 6 - Einbindung des Menschen, reibungslos und sicher

Cameron stellt bei seiner Gesetzmäßigkeit 6 „Human Integration" insbesondere auf die Absicherung der Integration des Menschen, d.h. auf Herausforderungen der kanal- und plattformübergreifenden Benutzerauthentifizierung mit dem Ziel der Vermeidung von Identitätsbetrügen ab. Dieser Punkt ist unweigerlich korrekt, hat jedoch in den vergangenen Jahren auf Grund einer Vielzahl neuer und ausreichend verlässlicher Absicherungsmechanismen (insbesondere biometrische) an Aufmerksamkeit verloren. Es verbleibt die Abwägung: Benutzerfreundlichkeit gegen Risiko.

Die Sicherheit eines Systems bei der Integration des Benutzers kann auf unterschiedliche Art und Weise erreicht werden: technisch, organisatorisch oder prozessual. Bei allen Abwägungen ist auf eine möglichst reibungslose Integration zu achten. Lassen sich sperrige Mehrfaktorauthentifizierungen ggf. vermeiden? Sind Konzepte der Hintergrund-

sicherheit, wie z. B. passive verhaltensbasierte Verfahren anwendbar? Kann die verwendete Authentifizierungsmethode kontextübergreifend vereinheitlicht und somit das Konzept des „Generalschlüssels“ tatsächlich umgesetzt werden?

Erfolgsfaktor 7 - Kontextübergreifend einheitliche User Experience

Über die Notwendigkeit einer simplen, schlüssigen und einheitlichen User Experience muss man bei digitalen Produkten gar nicht mehr viel erzählen. Wie heute beispielsweise der Zahlprozess bereits größtenteils zu einem one-click-Prozess minimalisiert, sollten auch die Identifikations-Prozesse möglichst einfach und schlank gehalten werden.

Gerade aber die Einheitlichkeit spielt bei e-Identity-Systemen eine bedeutende Rolle auf Grund der unterschiedlichen Kontexte, in denen sie verwendet werden. Die Benutzerführung und das Nutzungserlebnis sollte stets zuordenbar und wiedererkennbar sein sowie den gleichen oder zumindest ähnlichen Mustern folgen, unabhängig vom konkreten Nutzungsszenario; sei es beim Online-Login auf einer Nachrichten-Website, bei der online durchgeführten Identifikation im Rahmen einer Kontoeröffnung oder aber auch bei der Authentifizierung zur Öffnung eines Leihfahrzeugs.

Die Benutzer müssen sich stehts darüber im Klaren sein, dass sie das jeweilige e-Identity-System verwenden und welche Aktion (z.B. Authentifizierung) von ihnen erfordert werden. Die User Experience sollte beim Login auf eine Website nicht grundlegend abweichen vom Login in ein Fahrzeug (im Mietprozess). Die Beachtung des Erfolgsfaktors 5 „Pluralismus der Betreiber und Technologien“ erzeugt an dieser Stelle unter Umständen besondere Herausforderungen.

Erfolgsfaktor 8 - Kontextspezifisches Persona-Konzept

Die Motivation der heutigen e-Identity-Systeme besteht überwiegend darin, einen Identitätsstandard für viele (idealweise alle) digitalen Anwendungsfälle zu schaffen. Auf Grund der Vielzahl der unterschiedlichen Kontexte, einhergehend mit unterschiedlichen Wahrnehmungen der Benutzer, wird die Akzeptanz, eine einzige Identität für all diese Anwendungsfälle zu verwenden sehr gering sein. Die alltägliche Recherche im Internet bzw. das Login auf neuen und bislang unbekannten Webseiten wird bei Verwendung der amtlich verifizierten Identität und ggf. mit hinterlegtem Zahlungsmittel ggf. zu einem Störgefühl führen. Dafür wird man mit einer stark reduzierten oder sogar bewusst falschen Identität nutzen wollen, und das fängt schon bei der E-Mail-Adresse an. Nicht umsonst erfreuen sich Anbieter von Fake Mail Accounts hoher Beliebtheit. Die Benutzer werden - sofern das e-Identity-System kontextübergreifend anwendbar ist - wählen wollen, mit welcher Identität sie tatsächlich unterwegs sind. Mögliche kontextabhängige Identitäten können grob wie folgt zusammengefasst werden:

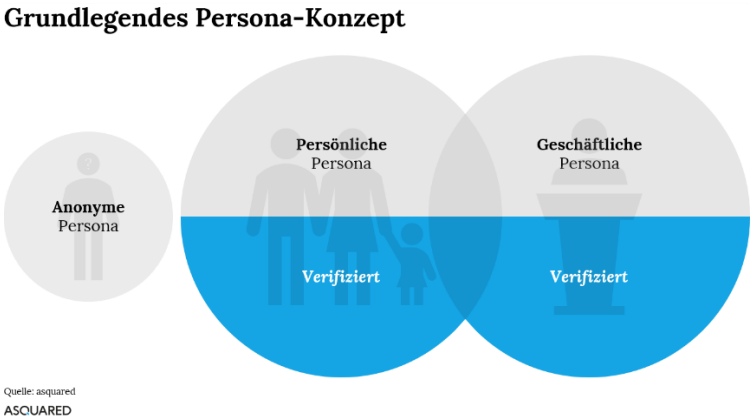

Abbildung 2: *Illustration grundlegendes Persona-Konzept*

Anonyme Persona – eine Identität mit selbsterklärte Identitätsdaten, die nicht notwendigerweise der Realität entsprechen, mit dem Ziel, keine realen Identitätsdaten preiszugeben. Anwendung finden diese beispielsweise bei registrierungspflichtigen Webseiten und -diensten, bei denen diese Identitätsdaten jedoch gar nicht geschäftsrelevant sind. Ein Beispiel ist die häufige Notwendigkeit, eine E-Mail-Adresse angeben zu müssen.

Persönliche Persona – eine Identität, die auf den realen Personendaten beruht. Diese sind zunächst selbsterklärt, der Benutzer hat jedoch ein Eigeninteresse, reale Daten anzugeben, da sie im Geschäftsprozess erforderlich sind. Beispiel: Name und Lieferadresse bei e-Commerce-Bestellungen. Betrugsfälle sind dadurch grundsätzlich nicht vermeidbar. Werden die Identitätsdaten von zertifizierter Stelle verifiziert, können diese auch für höherwertige Anwendungsfälle genutzt werden. Werden gar zertifizierte Identitätsmittel integriert (z.B. der digitale Personalausweis), so sind damit auch Geschäftsfälle möglich, die GwG-konforme Identifizierungen erfordern.

Geschäftliche Persona – ist eine Identität, die im Wesentlichen identifizierende Informationen zu einer Person in seinem beruflichen Kontext vorhält, wie beispielsweise die aktuelle Beschäftigungssituation bzw. sogar den gesamten Lebenslauf sowie berufliche Kontaktdaten. Es besteht eine Schnittmenge mit der persönlichen Persona – zumindest beim Attribut Name. Auch hier könnten diese Identitäten verifiziert werden. So ließen sich beispielsweise branchen- oder unternehmensweite Netzwerke bilden, Firmeneinkäufe gepoolt abwickeln oder firmeninterne Services nutzen (Nutzung Abteilungsfahrzeuge o.ä.).

Sehr wahrscheinlich bilden sich auch weitere differenziertere Personas heraus. Je nach Einsatzweite des e-Identity-Systems wird es Benutzer geben, die alle Personas nutzen werden, andere nutzen Kontext-fokussiert lediglich eine bestimmte Persona usw. Die Benutzer haben so die Wahl und können bestimmen, welche ihrer Identitäten genutzt werden soll und wie viel Information über diese Identität preisgegeben wird.

Ein e-Identity-System sollte das Persona-Konzept konsequent umsetzen, um dadurch die Selbstbestimmung der Benutzer im Einklang mit Erfolgsfaktor 1 „Kontrolle und Zustimmung durch den Nutzer“ herauszustellen.

Erfolgsfaktor 9 - Omnipräsente Anwendbarkeit

Ein e-Identity-System kann alle bisherigen Erfolgsfaktoren beachten; so lange es jedoch keine durchdringende Verbreitung erlangt, wird es nicht erfolgreich sein. Zur Etablierung als ein de-facto-Identitätsstandard ist eine Omnipräsenz für die Benutzer anzustreben und das sowohl kontext- als auch kanalübergreifend.

Kontextübergreifende Präsenz

Die Herausforderung liegt wie bei fast allen Neuprodukten – hier jedoch mit besonderer Relevanz - in der Lösung des Henne-Ei-Problems. Die ersten 8 Erfolgsfaktoren fokussieren überwiegend auf die Benutzerakzeptanz. Um kontextübergreifend bei möglichst vielen Akzeptanzstellen als Identifizierungsinstrument gelistet zu werden, muss auch den Akzeptanzvoraussetzungen auf Seiten der jeweiligen Service Provider Rechnung getragen werden. Dazu zählen insbesondere:

1 *Funktionalität je Kontext* – Die unterschiedlichen Kontexte in den unterschiedlichen Branchen bzw. Industrien stellen unterschiedliche Anforderungen an die Features der Identitätslösung. Die Funktionalität einer spezialisierten GwG- oder LOA4-konformen Lösung ist für eine Vielzahl der alltäglichen online-Anwendungen gar nicht erforderlich. Eine reine Single-Sign-On Lösung hingegen ist für e-Government Anwendungsfälle ungenügend. Es kommt also darauf an, Lösungen mit modularem und diversifiziertem Funktionsumfang zu etablieren.

2 *Potentielle (realistische) Benutzerreichweite* – Für ein Neuprodukt ist es immer schwierig, direkt mit hohen Nutzerzahlen zu punkten. So ist es jedoch um so wichtiger, keinerlei Akzeptanzhürden für die Benutzer zuzulassen und keinerlei Benutzergruppen auszuschließen. Gerade bei Identitätslösungen und der einhergehenden Vertrauensnotwendigkeit ist die Unabhängigkeit von einzelnen Anbietern wichtiger Erfolgsfaktor. Ebenso die Einfachheit bei der Benutzerregistrierung; idealerweise können bestehende Identitäten übernommen werden. Die Teilnahme großer Unternehmen mit großem Kundenstamm allein ist kein Erfolgsgarant. Immer wieder hört man „wir bringen direkt x Mio. Kunden mit“. Diese entscheiden aber selbst und wollen überzeugt werden. Das Etablieren neuer digitaler Lösungen in bislang unerschlossenen Kontexten mit direktem Mehrwert für den Kunden ist hier daher Mittel der Wahl.

3 *Kosten* – Weitere nichtfunktionale Reichweitekiller sind die Kosten und organisatorische Hürden (siehe Punkt 4). Identitätslösungen sind, wann immer es sich

lediglich um unverifizierte Identitätsdaten handelt (Single-Sign-On, selbsterklärte Daten), nicht bepreisbar, einzig LOA4-Funktionalitäten werden sich realistisch berechnen lassen. Für E-Identity-Systeme wird sich daher mit der Identitätsfunktionalität allein kein dunkelgrüner Business Case rechnen lassen. Für Service Provider wird es nahezu unentgeltlich sein müssen und es gilt, alternative Geschäftsmodelle zu Grunde zu legen.

4 *Vertragskonstrukt und SLAs etc.* – Idealerweise ist zur Teilnahme an einem e-Identity-System lediglich ein Teilnahmevertrag erforderlich. In der Realität wird das jedoch auf Grund des Pluralismus der Betreiber (Erfolgsfaktor 5) oder je nach Gesellschafterstruktur auf Grund des Wettbewerbs- und Kartellrechts nicht so einfach sein. In diesem Fall jedoch wird es unabdingbar sein, dafür Sorge zu tragen, dass marktkonforme Konzentrator- und Vermittlermodelle existieren, um das vertragliche Onboarding insbesondere mittelständischer und kleinerer Player zu erleichtern.

Kanalübergreifende Präsenz

Neben der kontextübergreifenden ist auch eine kanalübergreifende Präsenz unabdingbar für die weitreichende Anwendbarkeit eines e-Identity-Systems. Multi Cross und Omnichannel sind hier die Stichworte. Nur so lässt sich sicherstellen, dass es tatsächlich weitreichend Anwendung finden kann.

Insbesondere neue Geschäftsmodelle sind zunehmend auf mobile Anwendbarkeit zugeschnitten, so z. B. im Mobilitätskontext oder auch im stationären Handel. Von einer Hochverfügbarkeit der Systeme geht man heutzutage ohnehin aus, in mobilen Anwendungsfällen von e-Identity-Systemen jedoch ist die ständige Verfügbarkeit ein besonderes Thema, weshalb die Lösungen auch Mechanismen umfassend sollten, die eine Offline-Fähigkeit ermöglichen.

Das System muss in diesem Zusammenhang grundsätzlich für Dritte offen sein und entsprechende Integrationsmöglichkeiten bieten. Die Funktionalität muss in dritte Apps oder auch in weitere Systeme (z. B. Kassen- oder Produktionssysteme) integrierbar sein.

Fazit

Auf Basis der Laws of Identity von Kim Cameron haben wir neun Erfolgsfaktoren für heutige e-Identity-Systeme zusammengefasst. Diese beziehen sich sowohl auf die Benutzerakzeptanz als auch auf die Akzeptanz auf Seiten der Service Provider; sie zu beachten, wird der Schlüssel zur Etablierung einer weitreichend akzeptierten, auch gegenüber dem außereuropäischen Wettbewerb kompetitiven und fortdauernden Lösung sein.

Es wird in diesem Zusammenhang sehr interessant zu sehen, wie sich die angekündigten Initiativen positionieren und welche der Punkte Beachtung finden. Besonders spannend wird aber auch, herauszufinden, welche der Punkte explizit nicht adressiert werden und zu sehen, wie diese stattdessen gelöst werden.

Neben diesen System-spezifischen Zielsystemen besteht die größte Herausforderung anbieterübergreifend darin, bestehende Digitalisierungslücken durch Formulierung innovativer Anwendungsfälle (auch unter Nutzung der dann verfügbaren e-Identity-Systeme) zu schließen, um somit einen für den Benutzer deutlich wahrnehmbaren Mehrwert zu schaffen. Omnipräsente digitale Identitäten sind ein Enabler für Cross Channel und Cross Domain Ansätze. Die Verbindung bestehender Anwendungsfälle, die zusätzliche Services zu den etablierten Produkten erst ermöglichen, wird jedoch nur mit einem Mindestmaß an anbieter- und branchenübergreifender Kooperation gelingen. Dann aber wird es auch für den Anwender endlich wirklich spannend.

Quellenangaben

1 Kim Cameron, The Laws of Identity, 11.05.2005, http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

2 Asquared - Innovations- und Technologie-Blog, E-Identity-Lösungen in Europa – Ein europäischer Vergleich, 15.02.2018, https://asquared.company/blog/e-identity-loesungen-in-europa-ein-europaeischer-vergleich-686/

3 Meedia, Transparenz-Offensive: Facebook startet neue Kampagne zu Datenschutz und Privatsphäre, 29.01.2018, http://meedia.de/2018/01/29/facebook-startet-neue-kampagne-zu-datenschutz-und-privatsphaere/

4 Datenschutzbeauftragter INFO, WeChat Goes West – Chinas Überwachungs-App kommt, 16.01.2018, https://www.datenschutzbeauftragter-info.de/wechat-goes-west-chinas-ueberwachungs-app-kommt/

5 The Verge, How WeChat came to rule China - The multipurpose messaging app is becoming the nation's ID system, 01.02.2018, https://www.theverge.com/2018/2/1/16721230/wechat-china-app-mini-programs-messaging-electronic-id-system

6 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), 27.04.2016, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32016R0679

7 Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 44, Gesetz zur Anpassung des Datenschutzrechts, an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (DSAnpUG-EU), 05.07.2017, https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf

Autoren

Dr. Andreas Windisch ist Managing Director bei asquared. Er ist Diplom-Informatiker und promovierter Ingenieur. Er wirkte in leitenden Positionen bei Automobil-, Technologie- und Beratungsunternehmen und verfügt über langjährige Erfahrungen im Bereich des IT-Transformationsmanagements, insb. im Banken- und Finanzdienstleistersektor.

Über asquared

Asquared ist eine Unternehmensberatung aus Berlin. Mittelpunkt der Arbeit ist die Erarbeitung praktischer Lösungsansätze für den regulatorisch, technologisch und/oder gesellschaftlich induzierten Wandel, verbunden mit der jeweilig unmittelbaren Anwendung und Bestätigung im industriellen Umfeld.

Unser Augenmerk liegt stets auf Business und Technologie und ihrem Wechselspiel. Von der Neuausrichtung der Strategie, über das (Re)Design von Produkten und Services bis hin zur Operationalisierung – wir gestalten die Veränderung. Auf allen Ebenen.

Ausgewählte Erkenntnisse dieser theoretischen und praktischen Forschungsarbeiten stellen wir in Form von Publikationen und Fachvorträgen einer breiteren Öffentlichkeit zur Verfügung.

asquared GmbH
Pappelallee 78/79
10437 Berlin - Deutschland

Telefon +49 (0) 30 22 66 79 60
E-Mail contact@asquared.team

asquared.company
asquared.blog
twitter.com/asquaredgmbh
instagram.com/asquaredgmbh
linkedin.com/company/asquared