CIO

CSO
FROM IDG

VON IDG
COMPUTERWOCHE
VOICE OF DIGITAL

DIE WICHTIGSTEN ERGEBNISSE

präsentiert von

auth0 okta

Ein aktuelles Studienprojekt von

IDG RESEARCH SERVICES

Studie
(C)IAM

Exklusiver Studienpartner

auth0

Auth0 Deutschland
eine Produkteinheit von Okta
https://auth0.com/de

Impressum

Studienkonzept / Fragebogenentwicklung:
Simon Hülsbömer, Matthias Teichmann

Endredaktion / CvD Studienberichtsband:
Simon Hülsbömer

Analysen / Kommentierungen: Oliver Schonschek

Hosting / Koordination Feldarbeit: Armin Rozsa

Artdirector & Grafik: Daniela Petrini, Reutte

Umschlaggestaltung unter Verwendung eines Farbfotos von © shutterstock.com / LuckyStep

Lektorat: Elke Reinhold, München

Herausgeber:

IDG Tech Media GmbH

Georg-Brauchle-Ring 23
80992 München
Telefon: +49 89 36086–0
E-Mail: info@idg.de

Vertretungsberechtigter: Jonas Triebel, Geschäftsführer

Handelsregister München: HRB 99110,
UID-Nr. DE 811257834

Weitere Informationen unter: www.idg.de

Win-win mit CIAM

Simon Hülsbömer,
Senior Project Manager

Wer in der digitalen Welt unterwegs ist, ob beruflich oder privat, hinterlässt Datenspuren. Jede noch so kleine Interaktion mit Unternehmen erzeugt Kontakt- und Identitätsdaten, die gesammelt, konsolidiert, ausgewertet und weiterverarbeitet werden. Die auf diese Weise rasant wachsende Menge an digitalen Identitäten macht neue Strukturen und Ansätze für das Identity- und Access-Management (IAM) notwendig. Der EU-Datenschutz sowie Governance- und branchenabhängige Compliance-Anforderungen lassen den Umgang mit dieser Datenflut gleichzeitig immer komplexer und abstrakter werden.

Es entstehen neue Konzepte und Systeme für kundenzentriertes IAM (Customer IAM, kurz CIAM genannt), die darauf abzielen, die Balance zwischen Sicherheit und reibungslosem Kundenerlebnis bei der Nutzung eines digitalen Dienstes zu lösen. Hauptanliegen sind die Migration der Nutzer von Altsystemen, die Unterstützung neuer Geräte, die Skalierbarkeit und die Sicherheit der Endnutzer.

Soweit die Theorie. Wie es in der Praxis aussieht, soll die vorliegende Studie zeigen. Ein zentrales Ergebnis: Es ist nicht unbedingt der Endnutzer bzw. Kunde, der bei CIAM im Vordergrund steht. So ermöglichen bisher beispielsweise nur knapp ein Fünftel der befragten Unternehmen mit dedizierter CIAM-Strategie ihren Kunden den einheitlichen Zugang für die Nutzung mehrerer Dienste (Single Sign-on) oder einen Social-Login in das Kundenkonto, also die Anmeldung über Dienste wie Google oder Facebook.

Statt Nutzerfreundlichkeit und einfacher Bedienbarkeit dominieren regulatorische Fragen und Themen rund um die IT-Infrastruktur die CIAM-Strategien in den Unternehmen. Das liegt vermutlich daran, dass CIAM-Projekte sehr häufig aus bereits bestehenden IAM-Strategien heraus entwickelt werden, und dass IAM-Verantwortliche zumindest teils auch in CIAM-Fragen den Hut aufhaben. Das kann den neuen, Endkunden-zentrierten Anforderungen nicht gerecht werden.

Die IT täte bei CIAM-Projekten gut daran, andere Fachbereiche wie Entwicklung und Marketing mit ins Boot zu holen, um den Erwartungen der Kunden und damit den Anforderungen einer zeitgemäßen Customer Journey besser gerecht werden zu können. Ziel sollte sein, dass jeder Kontakt mit der Marke mit einem positiven Kundenerlebnis verbunden ist. Und dieses Prinzip ein Stück weit auch auf die „klassischen" IAM-Projekte zu übertragen, die die eigenen Mitarbeiter als „Kunden" im Fokus haben, würde womöglich helfen, die Prozesse weniger abstrakt und damit nutzerfreundlicher zu gestalten. Eine klassische Win-win-Situation also.

Ich wünsche Ihnen eine interessante Lektüre.

CIAM – besser die Kundenbrille aufsetzen

Eugenio Pace,
CEO Auth0

Die Deutschen sind Leute in Lederhosen und Dirndl, mit wenig Humor, einem Hang zu Bier und Autos und großem Arbeitswillen. Soweit das Klischee. Aber ist das wirklich die deutsche Identität? Das kann man erst mit Bestimmtheit sagen, wenn man weiß, ob eine Person wirklich diejenige ist, die zu sein sie vorgibt. Die Fachwelt spricht in diesem Zusammenhang von Customer Identity and Access Management, kurz CIAM.

Auth0 beauftragte IDG mit einer Trendstudie, die der zentralen Frage nachging, wie die IT- und Sicherheitsverantwortlichen in den Unternehmen auf das Management von vielfältigen digitalen Kundenidentitäten schauen. Was ist relevant für sie heute und in Zukunft, welche Ableitungen treffen sie, um die Voraussetzungen für ein wirksames CIAM zu schaffen? Und mit wem sollten sie bei diesem Thema dringend zusammenarbeiten?

Die Studie gibt Ihnen konkret Aufschluss darüber, wie Ihre Anwendungsfälle (Use Cases) des Identitätsmanagements aussehen sollten, um den richtigen Nährboden für eine erfolgreiche CIAM-Strategie zu schaffen. Sie erfahren ebenfalls, wann IAM-Systeme an ihre Grenzen geraten und last, but not least geht es darum, die Zusammenarbeit mit den Softwareentwicklern, dem Produktmanagement sowie dem digitalen Marketing zu suchen.

Auth0 möchte Ihnen mit dieser Studie einen fundierten Leitfaden an die Hand geben, der Ihnen die kritischen Erfolgsfaktoren dafür liefert, die Organisation der Identitäten von Mitarbeitern klar vom Management der digitalen Kundenidentitäten zu unterscheiden. Aber andererseits auch zu verstehen, wie aus IAM leicht CIAM werden kann.

Schon jetzt kann ich Ihnen verraten, einige Ergebnisse werden erwartbar für Sie sein, andere überraschend. In jedem Fall ist es ratsam, die eigene Perspektive zu wechseln und auf fachübergreifende Zusammenarbeit zu setzen.

Ich wünsche Ihnen viel Spaß bei der Lektüre.

Inhalt

Die wichtigsten Ergebnisse

Blick in die Zukunft

Studiendesign

Management Summary

Die Key Findings im Überblick

Der Kunde kommt in CIAM-Strategien noch zu kurz

Kriterien, die insbesondere den **Kunden im Fokus** haben, spielen bei weniger als 30 Prozent der Befragten eine Rolle. **Compliance und Infrastruktur** dominieren dagegen die CIAM-Strategien bei mehr als zwei Drittel der Unternehmen.

Die IT vermisst Wissen zu CIAM, das Marketing nicht

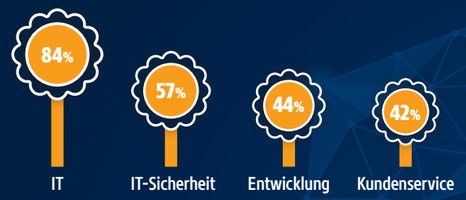
Während die **IT-Bereiche** zu 46 Prozent einen Know-how-Mangel bei CIAM befürchten, sorgen sich die **Fachbereiche** wegen fehlender kundenzentrierter Dienste, IT-Sicherheits-problemen und zu knappem Budget.

Kundenzugriffe über IAM-Systeme sind keine Ausnahme mehr

61 Prozent der Unternehmen berichten von **Zugriffen interner Beschäftigter** über ein Identitätsmanagement, 41 Prozent von entsprechenden **Zugriffen ihrer Kunden**.

Kundendaten dominieren die Verarbeitung in IAM-Systemen

Unternehmen mit IAM-System verarbeiten darin in 70 Prozent der Fälle Kundendaten. Bei **Unternehmen, deren Kunden Zugriff auf IT-Lösungen des Unternehmens besitzen**, steigt der Anteil sogar auf 83 Prozent. Bei Mitarbeiterdaten sind es insgesamt 63 Prozent, bei CIAM-Nutzern 68 Prozent.



84 Prozent sehen die IT als Entscheider bei der CIAM-Strategie

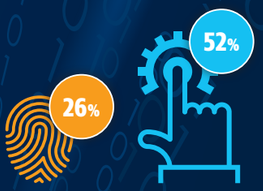
Nicht Entwicklung, Kundenservice, Vertrieb oder Marketing liegen auf Platz 2 der **Entscheider für CIAM,** sondern die IT-Sicherheit mit 57 Prozent. Die Entwicklung folgt auf Platz 3 mit 44 Prozent, der Kundenservice auf Platz 4 mit 42 Prozent.

Unternehmen, deren Kunden über IAM zugreifen, nutzen oder wollen die Cloud

Nur fünf Prozent der Unternehmen, deren **Kunden über ein IAM Zugriff** haben, lehnen die Cloud als IAM-Basis ab. Bei den Unternehmen insgesamt sind es mit acht Prozent nur wenig mehr. Damit bildet die Cloud eine wichtige Basis des IAM und noch mehr für CIAM.

Kundenidentitäten machen IT-Sicherheit noch wichtiger

86 Prozent der Unternehmen halten die **Absicherung digitaler Geschäftsprozesse** gegen Daten- oder Identitätsdiebstahl für wichtig. Bei Unternehmen, deren **Kunden über ein IAM Zugriff haben**, steigt der Anteil auf 93 Prozent. Der Blick auf Kunden erhöht also die Bedeutung von IT-Sicherheit.



52 Prozent glauben an Passwörter, nur 26 Prozent an Fingerprints

Moderne Verfahren der Authentifizierung wie **Fingerprint-Reader** haben nach Ansicht der Unternehmen weniger Zukunft als der **Passwort-Klassiker, PINs oder Sicherheitsfragen**. Das gilt selbst für die Unternehmen, deren Kunden über ein IAM auf die Unternehmens-IT zugreifen.

30 Prozent der IAM-Nutzer sehen Authentifizierung als Treiber im CIAM

Nur vier Prozent sehen die Cloud-Migration als Treiber im CIAM in den nächsten fünf Jahren. Nach den neuen Authentifizierungsmethoden sind es mit 26 Prozent die **Datenschutzvorschriften** und mit 25 Prozent die **Cyberbedrohungen**.

Unternehmen sehen vermehrt Risiken durch IAM-Implementierungsfehler

Unternehmen, die Cyberattacken als Treiber für CIAM in den nächsten fünf Jahren einstufen, nennen zu 60 Prozent **Injection Attacks**, zu 54 Prozent **Credential Stuffing-Angriffe** und zu 27 Prozent **Account Creation Attacks**.

1

Der Kunde kommt oft zu kurz

69 Prozent* der befragten Unternehmen nennen IT-Infrastrukturen und IT-Sicherheit als Kriterien ihrer Strategie im CIAM. Einen einheitlichen Zugang für Kunden bei Nutzung mehrerer Dienste berücksichtigen dagegen nur 22 Prozent in ihrer CIAM-Strategie. Die Möglichkeit für ein Social-Login beim Kundenkonto sehen nur 19 Prozent vor.

Während die Fachbereiche zu 33 Prozent einheitliche Kundenanmeldungen für mehrere Dienste als Teil der CIAM-Strategie erachten, ist dies im IT-Bereich nur bei 21 Prozent der Befragten so, unter den Befragten aus Geschäftsführung und Vorstand sogar nur zu 11 Prozent.

Offensichtlich dominieren unter den Kriterien solche, die auch bei einer klassischen IAM-Strategie relevant sind, wie Authentifizierung, Registrierung, Compliance, Datenschutz und Risiko-Management, das immer noch für 49 Prozent der Befragten als Kriterium eine Rolle spielt.

Anforderungen, die sich speziell auf Kundenbindung, Customer Journey, einheitliche Erfahrung für alle Marken, einheitlichen Zugang für den Kunden zur Nutzung mehrerer Dienste und auf Marketing-Automation beziehen, erreichen maximal 29 Prozent der Nennungen.

Dies legt den Schluss nahe, dass die Mehrheit der befragten Unternehmen von ihrer bestehenden IAM-Strategie aus versuchen, CIAM umzusetzen. Die IAM-Strategie obliegt in vielen Unternehmen aber dem IT-Bereich und ist kein Thema, mit dem sich Fachbereiche wie die Entwicklung oder das Marketing befassen, obwohl sich gerade das Marketing um die Implementierung der Customer Journey kümmern muss.

Damit die Kundenaspekte in der CIAM-Strategie eine stärkere Rolle spielen, erscheint es deshalb sinnvoll, weitere Unternehmensbereiche neben dem IT-Bereich einzubeziehen.

Welche Kriterien enthält Ihre CIAM-Strategie?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, bei denen eine dedizierte CIAM-Strategie vorhanden ist. Basis: n = 184

IT-Infrastruktur (Authentifizierung, Registrierung)	68,5
IT-Sicherheit (Compliance, Datenschutz)	68,5
Risiko-Management	48,4
Zeitplan hinsichtlich CIAM-Umsetzung	44,0
Login-Validierung	35,3
Zentralisierte Daten	34,8
Gesetzeskonforme Nutzung von Kundenidentitäten	33,2
Marketing (Kundenbindung/Customer Journey)	28,8
Einheitliche Erfahrung für alle Marken	25,5
Einheitlicher Zugang für den Kunden zur Nutzung mehrerer Dienste	21,7
Marketing-Automation (Social Login beim Kunden-Konto)	18,5

* Um den Anforderungen an eine valide Studie gerecht zu werden, wurden insgesamt 288 qualifizierte Interviews mit (IT-)Verantwortlichen in Unternehmen der DACH-Region aus allen Unternehmensbereichen (C-Level, IT, Fachbereiche) und aus allen Branchen durchgeführt.

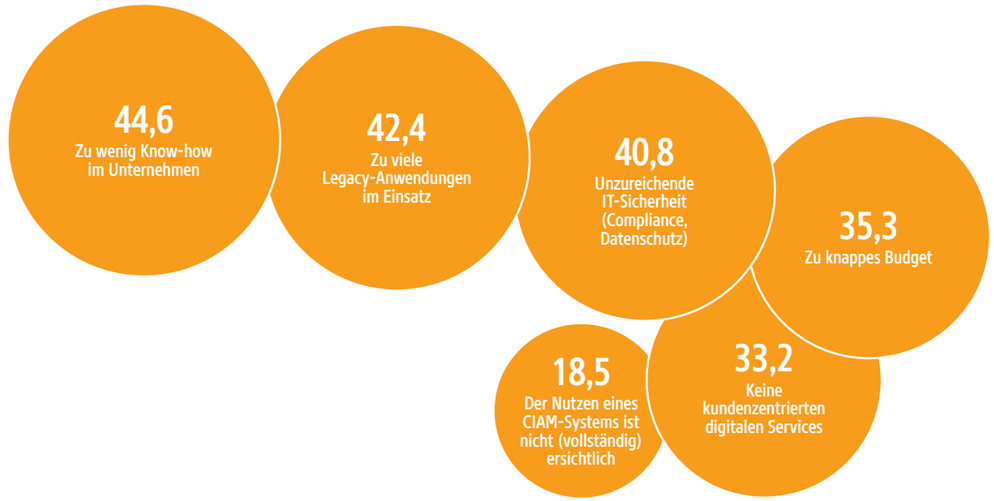
2

Angst vor Know-how-Mangel

45 Prozent der Unternehmen haben die Sorge, zu wenig Know-how im Unternehmen zur Umsetzung ihrer CIAM-Strategie zu haben. 42 Prozent haben Bedenken, dass sie zu viele Legacy-Anwendungen im Einsatz haben. Eine unzureichende IT-Sicherheit bei der Umsetzung von CIAM fürchten 41 Prozent. Einen zu geringen Nutzen bei CIAM sehen dagegen nur 19 Prozent.

Was sind Ihre größten Bedenken hinsichtlich der Umsetzung der CIAM-Strategie?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, bei denen eine dedizierte CIAM-Strategie vorhanden ist. Basis: n = 184



Während 51 Prozent der CIOs, Technik-Vorstände und CISOs das Know-how im Unternehmen als zu gering ansehen, wenn es um die Umsetzung von CIAM geht, sinken diese Bedenken im IT-Bereich auf 46 Prozent und in der Geschäftsführung sogar auf elf Prozent.

Fachbereiche wie das Marketing nennen den Know-how-Mangel überhaupt nicht als Problem bei der Umsetzung von CIAM. Sie sorgen sich zu 67 Prozent um die IT-Sicherheit und um das Fehlen kundenzentrierter digitaler Services. Jeder dritte Befragte aus den Fachbereichen hat zudem Bedenken wegen eines zu knappen Budgets.

Unter den CIOs, Technik-Vorständen und CISOs zweifeln 23 Prozent am Nutzen von CIAM, in der Geschäftsführung 17 Prozent und im IT-Bereich 13 Prozent.

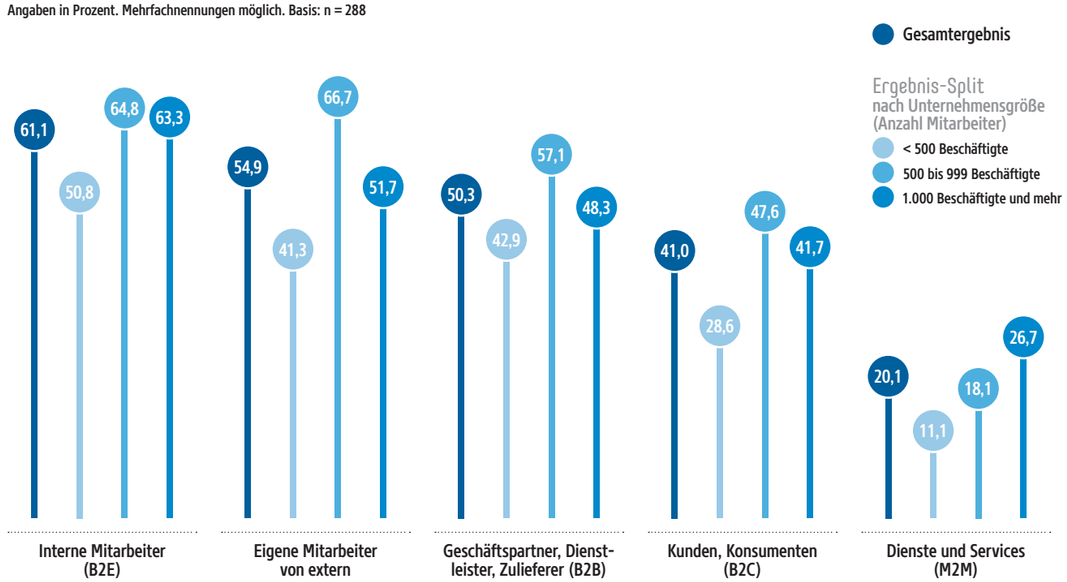
Bedenkt man aber, dass es der IT-Bereich ist, der aktuell noch in den meisten Fällen für die CIAM-Strategie verantwortlich zeichnet, muss der befürchtete Know-how-Mangel zu denken geben. Auch hier erscheint es empfehlenswert, Fachbereiche wie das Marketing einzubeziehen, da dort kein Mangel an notwendigem Fachwissen beklagt wird.

Der gefürchtete Know-how-Mangel im IT-Bereich könnte auch mit einem Mangel an Entwickler-Ressourcen verbunden sein, die die Kundenapplikationen entwickeln und umsetzen können. In diesem Fall müsste der IT-Bereich das entsprechende Budget für Entwickler-Ressourcen freigeben und könnte so den Know-how-Mangel mindern oder beseitigen.

3

Wer (oder was) greift über Authentifizierungs- und Identitätsmanagement-Tools auf Systeme Ihres Unternehmens zu?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 288



IAM-Bedarf im Endkundengeschäft wächst

Zumeist sind es zwar eigene Mitarbeiter, die über Identitätsmanagement-Tools auf IT-Systeme des Unternehmens zugreifen (61 Prozent interne, 55 Prozent externe Zugriffe) oder Partner und Lieferanten (50 Prozent). In 41 Prozent der Firmen gehen derartige Zugriffe aber bereits von Kunden aus.

Unternehmen, die sich für Kundenzugriffe über ein IAM geöffnet haben, berichten allesamt über eine entsprechende Nutzung. Auch bei den internen Beschäftigten, bei den Partnern und Lieferanten und bei den Maschinen finden bei diesen Unternehmen mehr Zugriffe über IAM-/CIAM-Lösungen statt. So berichten die CIAM-Nutzer zu 64 Prozent von internen und von externen Zugriffen der Beschäftigten, zu 57 Prozent von Partnerzugriffen und zu 28 Prozent von M2M-Zugriffen über IAM-Lösungen.

Zugriffe von Endkunden werden mit 48 Prozent besonders häufig von Unternehmen mit 500 bis 999 Beschäftigten beschrieben, bei weniger als 500 Beschäftigten sind es nur noch 29 Prozent, ab 1.000 Beschäftigten dagegen 42 Prozent.

Auch das jährliche IT-Budget wirkt sich darauf aus, wie häufig von Kunden berichtet wird, die über eine Identitätsmanagement-Lösung auf die IT des Unternehmens zugreifen. Sind es 38 Prozent bei den Unternehmen mit weniger als zehn Millionen Euro IT-Budget pro Jahr, die von Kundenzugriffen berichten, steigt der Anteil auf 46 Prozent bei einem jährlichen IT-Budget ab zehn Millionen Euro.

Berücksichtigt werden sollte dabei, dass sich der interne Zugriff auf IAM-Systeme von den externen Zugriffen durch Endnutzer unterscheidet, da diese von ganz unterschiedlichen Plattformen und Geräten aus erfolgen können und häufiger wechselnde Zugangsdaten (E-Mail) haben.

4

Vor allem Kundendaten werden mittels IAM-Tools verarbeitet

In IAM-Lösungen werden in 70 Prozent der Unternehmen Kundendaten verarbeitet, bei 63 Prozent Mitarbeiterdaten und bei 58 Prozent Partnerdaten. Geschäfts- und Vertragsdaten nennen 58 Prozent und Maschinen- und Sensordaten noch 25 Prozent. Bei Unternehmen, deren Kunden über ein IAM zugreifen, sind es sogar 83 Prozent, die Kundendaten im Identitätsmanagement verarbeiten.

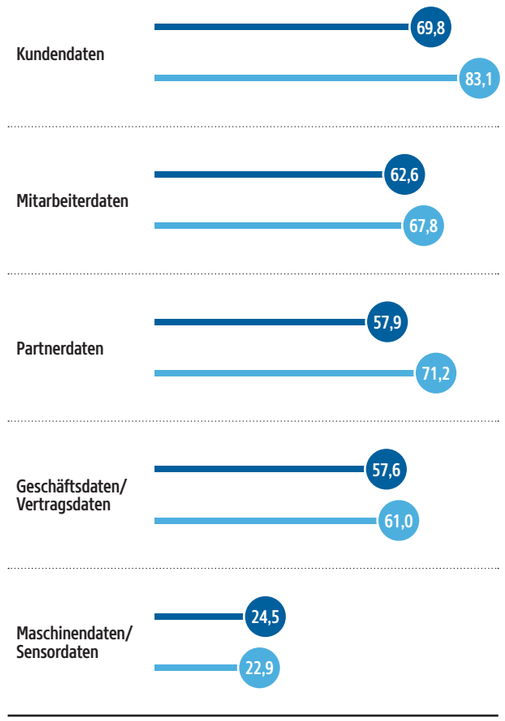
Kundendaten dominieren die Datenverarbeitung in IAM-Systemen, auch dann, wenn man nicht nur die Unternehmen betrachtet, die Kundenzugriffe auf ihr IAM erlauben.

Gerade bei mittelgroßen Unternehmen mit 500 bis 999 Beschäftigten werden Kundendaten in den IAM-Systemen verarbeitet, hier sind es 75 Prozent. Bei größeren Unternehmen mit 1.000 und mehr Beschäftigten sinkt der Anteil auf 66 Prozent, bei kleineren Unternehmen mit weniger als 500 Beschäftigten auf 68 Prozent.

Das IT-Budget, das pro Jahr zur Verfügung steht, hat ebenfalls einen gewissen Einfluss darauf, wie verbreitet die Verarbeitung von Kundendaten in IAM-Systemen ist. Kleinere IT-Budgets bedeuten nicht automatisch, dass Kundendaten weniger häufig im IAM verarbeitet werden, im Gegenteil. Bei einem jährlichen IT-Budget von bis zu zehn Millionen Euro sind es 71 Prozent, die Kundendaten im IAM verarbeiten. Steigt das IT-Budget, sinkt der Anteil leicht auf 69 Prozent.

Welche Arten von Daten werden in Ihrem Unternehmen mittels IAM-Services verarbeitet?

Angaben in Prozent. Mehrfachnennungen möglich.



Unternehmen, bei denen ein on-Premises-gestütztes und/oder cloudbasiertes Identity- und Access-Management (IAM) zum Einsatz kommt.
Basis: n = 278

Filter: Unternehmen, bei denen Kunden und/oder Konsumenten (B2C) über Authentifizierungs- und Identitätsmanagement-Tools auf Systeme des Unternehmens zugreifen.
Basis: n = 118

Man kann daraus schließen, dass es bei der überwiegenden Mehrzahl der Unternehmen ein großes Potenzial für CIAM gibt, da sie bereits in ihrem IAM-System Kundendaten vorhalten.

5

IT-Bereich und Security dominieren die CIAM-Strategie

84 Prozent der Unternehmen nennen den IT-Bereich als Entscheidungsinstanz für die CIAM-Strategie, 57 Prozent die IT-Sicherheit. Die Entwicklung, die zum Beispiel neue Funktionen zur Kundenauthentifizierung in die Strategie einbringen könnte, nennen dagegen nur 44 Prozent, den Kundenservice 42 Prozent und die Rechtsabteilung 16 Prozent.

Unternehmen, die mit weniger als 500 eine geringere Zahl von Beschäftigten haben, nennen den IT-Bereich als Entscheider in der CIAM-Strategie besonders häufig, hier sind es 89 Prozent. Bei 500 bis 999 Beschäftigten sinkt der Anteil derer, die die IT-Abteilung für entscheidend im CIAM sehen, auf 82 Prozent, bei 1.000 und mehr Beschäftigten steigt der Anteil wieder leicht auf 84 Prozent.

Die IT-Sicherheit hingegen nennen die Unternehmen mit weniger als 500 Beschäftigten besonders selten, hier sind es nur 33 Prozent, bei 500 bis 999 Beschäftigten dagegen 68 Prozent und ab 1.000 Beschäftigten 54 Prozent.

Die Entwicklung ist den kleineren Unternehmen dagegen wieder wichtiger als den größeren. Der Anteil der Unternehmen, die die Entwicklung als entscheidend für CIAM betrachten, liegt bei weniger als 500 Beschäftigten bei 61 Prozent, bei Unternehmen mit 500 bis 999 Beschäftigten bei 48 Prozent und ab 1.000 Beschäftigten bei 34 Prozent.

Vergleicht man die Bedeutung, die dem IT-Bereich und der IT-Sicherheit für CIAM beigemessen wird, mit den Kriterien, die die Unternehmen für die CIAM-Strategie nennen, so deckt sich dies. Auch hier sind kundenbezogene Kriterien weniger im Fokus.

Die starke Gewichtung von IT und IT-Sicherheit als Entscheider in der CIAM-Strategie kann dazu führen, dass CIAM-Projekte aus einem bestehenden IAM-Projekt begonnen werden, da bei IAM die IT stark involviert ist. Klassische IAM-Lösungen würden dann für CIAM-Vorhaben eingesetzt, ohne jedoch die dafür notwendigen Funktionen bieten zu können, die CIAM im Gegensatz zu IAM benötigt. Dazu gehört zum Beispiel die Unterstützung vielfältiger Plattformen und Endgeräte, die Kunden einsetzen können.

Bereiche mit Kundenkontakt und die Entwicklung sind bislang weniger präsent in den CIAM-Entscheidungen, was dazu führen kann, dass neue Funktionen und der Kundenfokus in den CIAM-Strategien zu kurz kommen können.

Die Empfehlung lautet deshalb, IT und IT-Sicherheit weiterhin eine hohe Relevanz zu verleihen, aber bei CIAM-Projekten stärker die Entwicklungsabteilung und die Kundenbereiche in die Entscheidungsrolle zu bringen. Dadurch kann man gewährleisten, dass zum Beispiel moderne Authentifizierungsverfahren, die sich die Kunden wünschen, in der CIAM-Strategie besser und schneller berücksichtigt werden, ohne Kompromisse bei der Sicherheit eingehen zu müssen.

5

Welche Unternehmensbereiche sind in die Entscheidungsprozesse rund um die CIAM-Strategie involviert?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, bei denen Kunden und/oder Konsumenten (B2C) über Authentifizierungs- und Identitätsmanagement-Tools auf Systeme des Unternehmens zugreifen. Basis: n = 118

	Gesamtergebnis	Ergebnis-Split nach IT-Budget		Ergebnis-Split nach Unternehmensgröße (Anzahl Mitarbeiter)		
		< 10 Mio. Euro	10 Mio. Euro und mehr	< 500 Beschäftigte	500 bis 999 Beschäftigte	1.000 Beschäftigte und mehr
IT	83,9	79,7	89,8	88,9	82,0	84,0
(IT-)Security	56,8	55,1	59,2	33,3	68,0	54,0
Produkt-Entwicklung (Forschung & Entwicklung)	44,1	49,3	36,7	61,1	48,0	34,0
Kundenservice	41,5	50,7	28,6	55,6	54,0	24,0
Vertrieb	37,3	37,7	36,7	50,0	42,0	28,0
Marketing	34,7	40,6	26,5	44,4	30,0	36,0
Rechtsabteilung	16,1	18,8	12,2	22,2	12,0	18,0
Andere Unternehmensbereiche	0,8	1,4	0,0	0,0	2,0	0,0

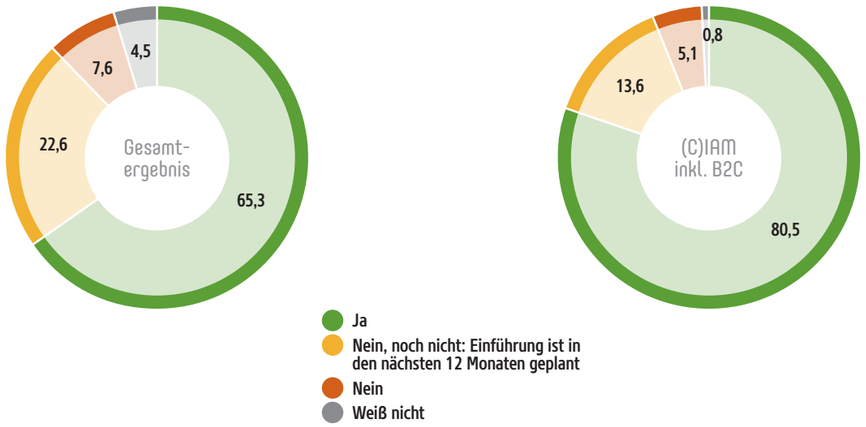
6

Cloudbasiertes IAM auf der Überholspur

81 Prozent der Unternehmen, deren Kunden mittels (C)IAM-Lösung auf interne Systeme zugreifen, setzen diese Tools auf Cloud-Basis ein, weitere 14 Prozent planen den Schritt in die Cloud binnen eines Jahres. Auch in den Unternehmen, die keine Kundenzugriffe auf ihr IAM erlauben, ist das cloudbasierte IAM stark im Kommen.

Gibt es in Ihrem Unternehmen ein cloudbasiertes Identity- und Access-Management (IAM)?

Gesamtergebnis: Angaben in Prozent. Basis: n = 288
(C)IAM inkl. B2C: Angaben in Prozent. Filter: Unternehmen, bei denen Kunden und/oder Konsumenten (B2C) über Authentifizierungs- und Identitätsmanagement-Tools auf Systeme des Unternehmens zugreifen. Basis: n = 118



65 Prozent aller befragten Unternehmen setzen eine cloudbasierte Lösung für das Identity and Access Management (IAM) ein. Weitere 23 Prozent planen dies innerhalb von zwölf Monaten. Gegen die Cloud haben sich acht Prozent entschieden, fünf Prozent haben noch keine entsprechende Entscheidung gefällt.

Besonders verbreitet sind cloudbasierte IAM-Lösungen bei Unternehmen mit 500 bis 999 Beschäftigten, die zu 69 Prozent eine Cloud-Lösung im IAM gewählt haben. Unternehmen mit weniger als 500 Beschäftigten arbeiten mit einem cloudbasiertem IAM in 60 Prozent der Fälle, bei mindestens 1.000 Beschäftigten sind es 65 Prozent. Die Höhe des jährlichen IT-Budgets hingegen beeinflusst den Cloud-Anteil unter den IAM-Lösungen nicht.

Der hohe Zuspruch für cloudbasierte Lösungen bei Unternehmen mit Kundenzugriffen über ein IAM sollte im Zusammenhang mit den Kriterien dieser Unternehmen gesehen werden. Diesen Unternehmen kommt es bei CIAM auch auf Kriterien an, die den Kunden in den Blick nehmen, wie Kundenbindung und Customer Journey sowie Skalierbarkeit, Sicherheit und Verfügbarkeit für Hunderttausende oder sogar Millionen Kunden, im Gegensatz zu Hunderten oder einigen Tausenden von Beschäftigten, die auf Workforce-IAM-Systeme zugreifen.

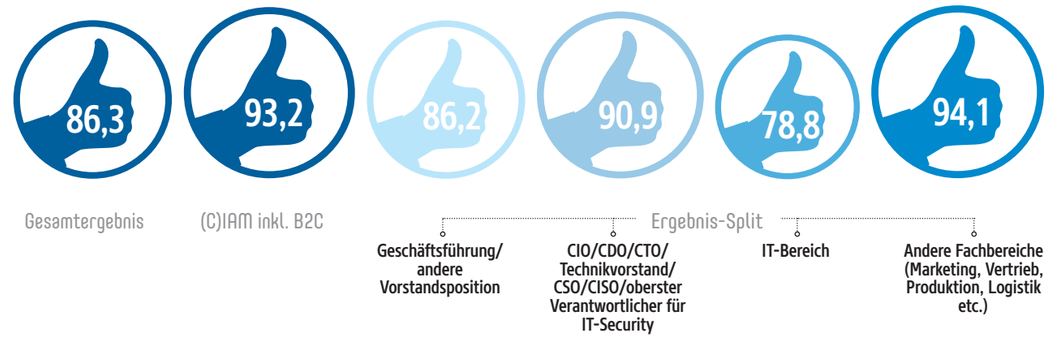
Tatsächlich kann man bei cloudbasierten Lösungen davon ausgehen, dass sich diese für Kunden einfacher nutzen lassen, da zum Beispiel keine lokalen Installationen auf Kundenseite dafür notwendig sind.

7

Wie wichtig ist für Ihr Unternehmen die Absicherung von digitalen Geschäftsprozessen vor Datendiebstahl bzw. dem Angriff auf digitale Identitäten?

Angaben in Prozent. Filter: Unternehmen, bei denen ein on-Premises-gestütztes und/oder cloudbasiertes Identity- und Access-Management (IAM) zum Einsatz kommt. Basis: n = 278

„Sehr wichtig / wichtig"



Top-Priorität Datensicherheit

Kein Unternehmen, das Zugriffe der Kunden über ein IAM vorsieht, sagt, dass die Absicherung digitaler Geschäftsprozesse gegen Daten- und Identitätsdiebstahl unwichtig sei. In den IT-Bereichen der insgesamt befragten Unternehmen sind es immerhin drei Prozent, die Datensicherheit als unwichtig bezeichnen.

Unter den befragten Unternehmen sagen 86 Prozent, dass die Absicherung von digitalen Geschäftsprozessen vor Datendiebstahl oder dem Angriff auf digitale Identitäten „wichtig" oder „sehr wichtig" ist. Dieser Wert steigt noch um sieben Prozentpunkte, wenn man speziell die Unternehmen ansieht, die Kundenzugriffe über ein IAM haben und sich damit speziell der Bedeutung der Kundenidentitäten bewusst sind.

Besonders wichtig ist die Absicherung gegen Daten- und Identitätsdiebstahl aus Sicht der Fachbereiche wie dem Marketing. Hier sind es 94 Prozent der Antworten. Unter den CIOs, Technik-Vorständen und CISOs sind es noch 91 Prozent, die die Datensicherheit für wichtig oder sehr wichtig halten. Bei der Geschäftsführung sinkt der Anteil auf 86 Prozent und in der IT-Abteilung sogar auf 79 Prozent.

Bedenkt man, dass IAM-Projekte vornehmlich im IT-Bereich gesteuert und CIAM-Vorhaben oft zuerst aus dem bestehenden IAM-Projekt heraus versucht werden, ist der vergleichsweise geringe Stellenwert der Absicherung eher bedenklich. Fachbereiche könnten in CIAM-Projekten damit nicht nur für mehr Kundenfokus sorgen, sondern auch die Bedeutung der Datensicherheit betonen.

Dabei sollte berücksichtigt werden, dass sich die Angriffe und damit auch die Anzeichen für Angriffe auf Kundenanwendungen unterscheiden von denen auf Applikationen, die die Beschäftigten nutzen.

Die Maßnahmen für Datensicherheit sollten deshalb auf die Risiken zugeschnitten sein, die bei Kundenapplikationen vorherrschen, und Lösungen umfassen, die Kunden akzeptieren. Eine adaptive, risikoabhängige Sicherheit ist der Weg der Wahl, um den Risiken bei Kundenapplikationen zu begegnen und bei Bedarf die jeweils notwendigen Sicherheitsmaßnahmen zu ergreifen.

Jedes zweite Unternehmen glaubt noch an das Passwort

Benutzername und Passwort, PIN und Sicherheitsfragen sind die Methoden, die die Unternehmen am häufigsten nennen, wenn es um die Verfahren der Authentifizierung in fünf Jahren geht. Bei Unternehmen mit Kundenzugriffen über ihr IAM werden Passwörter von 52 Prozent, PINs von 42 Prozent und Sicherheitsfragen von 39 Prozent genannt. Fingerabdruck-Scans sehen dagegen nur 26 Prozent.

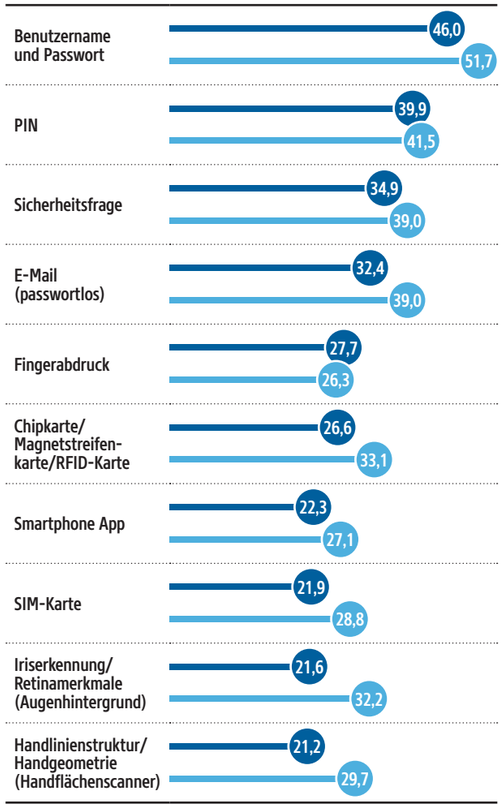
Betrachtet man die Fingerabdruck-Scans als Beispiel für neuere Verfahren der Authentifizierung, stellt man fest, dass 47 Prozent der Fachbereiche dieses Verfahren in fünf Jahren im Einsatz sehen, der IT-Bereich jedoch nur zu 24 Prozent. In der Geschäftsführung, bei den CIOs, Technik-Vorständen und CISOs hat der Fingerabdruck mit 28 Prozent etwas mehr Anhänger.

Interessanterweise sind es die Unternehmen mit dem kleineren IT-Budget von weniger als zehn Millionen Euro pro Jahr, die die Fingerabdruck-Scans zu 30 Prozent als Verfahren der Zukunft sehen. Steigt das jährliche IT-Budget auf mehr als zehn Millionen Euro, sind es nur noch 24 Prozent der Unternehmen. Man kann daraus schließen, dass die Einführung neuer Verfahren zur Authentifizierung eher keine Frage des IT-Budgets ist. Stattdessen geht es vielmehr darum, dass es zu wenig Entwickler-Ressourcen in den Unternehmen gibt und die vorhandenen Entwicklungsabteilungen nicht umfassend eingebunden werden.

Eine aktuelle YouGov-Verbraucherstudie in Zusammenarbeit mit Auth0 zeigt, dass Unternehmen die Erwartungen ihrer Kunden im Bereich der Authentifizierung noch zu wenig kennen. Die ständige Suche nach neuen starken Passwörtern führt zu Abbrüchen bei

Was meinen Sie, welche Methoden zur Authentifizierung von Nutzern werden in fünf Jahren in Ihrem Unternehmen zum Einsatz kommen?

Angaben in Prozent. Mehrfachnennungen möglich.
Dargestellt sind die Top-10 Nennungen.



Unternehmen, bei denen ein on-Premises-gestütztes und/oder cloudbasiertes Identity- und Access-Management (IAM) zum Einsatz kommt. Basis: n = 278

Unternehmen, bei denen Kunden und/oder Konsumenten (B2C) über Authentifizierungs- und Identitätsmanagement-Tools auf Systeme des Unternehmens zugreifen. Basis: n = 118

Neuregistrierungen für Online-Dienste, ebenso wie zu komplizierte, langwierige Anmeldungen den Kaufvorgang abbrechen lassen können.

Es scheint empfehlenswert, dass die Unternehmen noch stärker die Kundenwünsche betrachten, wenn sie die Verfahren der Authentifizierung planen.

Neue Authentifizierungstechnologien werden zu CIAM-Treibern

Fast jedes dritte Unternehmen (30 Prozent) mit IAM-Lösung stuft die neuen Authentifizierungsverfahren als Treiber im CIAM der nächsten fünf Jahren ein. 26 Prozent bezeichnen den Datenschutz als Treiber, 25 Prozent die Cyberbedrohungen. Unternehmen, deren Kunden über eine IAM-Lösung zugreifen, stufen die Authentifizierungsmethoden mit 39 Prozent sogar als noch wichtiger ein.

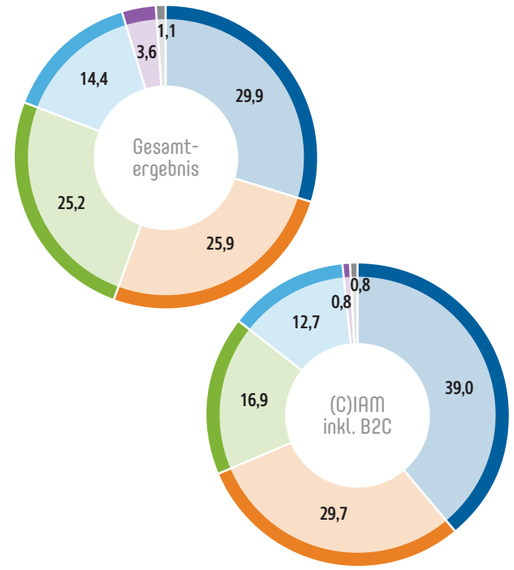
Während die Cloud-Migration nur von vier Prozent als Treiber im CIAM der nächsten fünf Jahre gesehen wird, nennen 14 Prozent die digitale Transformation an sich als treibenden Faktor. Unternehmen mit Kundenzugriffen über ihre IAM-Lösung stufen die Datenschutzvorschriften mit 30 Prozent höher ein, dafür aber die Cyberbedrohungen mit 17 Prozent niedriger im Vergleich zum Durchschnitt aller Unternehmen mit IAM-Lösung.

Besonders die Geschäftsführung und der Vorstand betonen mit 38 Prozent die treibende Kraft der Authentifizierungsmethoden für CIAM. Für den IT-Bereich sind es dagegen besonders die Cyberbedrohungen, die mit 27 Prozent überdurchschnittlich oft als Treiber genannt werden.

Erneut zeigt sich, dass der IT-Bereich neue Funktionen wie die biometrische Authentifizierung als weniger entscheidend ansieht als zum Beispiel den Schutz vor Cyberattacken. Dabei spielen die neuen Authentifizierungsverfahren durchaus eine wichtige Rolle, wenn es um einen höheren Schutz bei gleichzeitig höherem Nutzerkomfort geht. Dies sollte bei den Strategiegesprächen zu CIAM stärker auf die Agenda gesetzt werden.

Was wird Ihrer Meinung nach der größte Treiber für die Einführung von CIAM in den nächsten fünf Jahren sein?

Angaben in Prozent.
Filter Gesamtergebnis: Unternehmen, bei denen ein on-Premises-gestütztes und/oder cloudbasiertes Identity- und Access-Management (IAM) zum Einsatz kommt.
Basis: n = 278
(C)IAM inkl. B2C: Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, bei denen Kunden und/oder Konsumenten (B2C) über Authentifizierungs- und Identitätsmanagement-Tools auf Systeme des Unternehmens zugreifen. Basis: n = 118



Neue Authentifizierungsmethoden/-technologien
Datenschutzvorschriften
Cybersicherheitsbedrohungen/-angriffe
Digitale Transformation
Migration in die Cloud
Weiß nicht

Das Ziel von CIAM sollte der Aufbau von Kundenvertrauen sein, in dem User Experience, Sicherheit und Datenschutz durch fortgeschrittene Authentifizierungstechnologien ausbalanciert werden.

Ein weiterer Punkt spricht für die Bedeutung moderner Authentifizierungstechnologien: So sollte der Endnutzer immer eine Auswahl unterschiedlicher Authentifizierungsmethoden haben, um sich je nach Situation und Login-Präferenzen anzumelden. Branchenspezifische Anforderungen spielen hier ebenfalls eine wichtige Rolle.

10

Injektionsangriffe und Credential Stuffing als relevanteste Cyberattacken

Unternehmen, die Cyberangriffe als Treiber für CIAM in den nächsten fünf Jahren sehen, nennen zu 60 Prozent Injection Attacks, 54 Prozent sehen die Relevanz von Credential-Stuffing-Angriffen und 27 Prozent die Account Creation Attacks. Mit 84 Prozent dominiert bei Vorständen und Geschäftsführern dagegen die Sorge vor Credential Stuffing.

Welche Art der aufgeführten Cybersicherheitsbedrohungen/-angriffe schätzen Sie als relevant ein?

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Unternehmen, die der Meinung sind, dass Cybersicherheitsbedrohungen in den nächsten fünf Jahren der größte Treiber für die Einführung von CIAM sein werden. Basis: n = 70

	Gesamtergebnis	Ergebnis-Split nach Unternehmensgröße (Anzahl Mitarbeiter)		
		< 500 Beschäftigte	500 bis 999 Beschäftigte	1.000 Beschäftigte und mehr
Injection Attacks: Cyberkrimelle führen beliebigen Code aus, um die Authentifizierungssysteme zu umgehen. Diese wirksamen Angriffe nutzen häufig anfällige Identitätsimplementierungen aus	60,0	52,4	54,5	70,4
Credential Stuffing-Angriffe: Cyberkriminelle nutzen gestohlene Benutzernamen und Kennwörter aus Unternehmen A, um auf Benutzerkonten von Unternehmen B zuzugreifen	54,3	52,4	59,1	51,9
Account Creation Attacks: Mithilfe einer großen Anzahl gefälschter Konten nutzen Cyberkriminelle Anmeldeboni aus, verbreiten Fehlinformationen oder richten anderen Schaden an.	27,1	23,8	27,3	29,6

Während Technik-Vorstände, CIOs und CISOs Credential-Stuffing-Angriffe mit 65 Prozent überdurchschnittlich oft als Risiko nennen, ist diese Angriffsmethode mit 41 Prozent in der IT und mit 33 Prozent in den Fachbereichen wie Marketing nur unterdurchschnittlich bewusst oder bekannt.

Mittelgroße Unternehmen mit 500 bis 999 Beschäftigten sehen Credential-Stuffing-Angriffe mit 59 Prozent überdurchschnittlich stark als relevantes Risiko. Dagegen nimmt die Relevanz dieser Angriffsform aus Sicht der Unternehmen ab, wenn das jährliche IT-Budget steigt.

So nennen 57 Prozent der Unternehmen mit einem jährlichen IT-Budget von weniger als zehn Millionen Euro die Credential-Stuffing-Angriffe, dagegen nur noch 47 Prozent bei einem jährlichen IT-Budget ab zehn Millionen Euro.

Bei den Angriffsformen Injection Attacks und Account Creation Attacks dagegen steigt die Relevanz, wenn ein höheres IT-Budget zur Verfügung steht, bei Injection Attacks von 59 Prozent auf 63 Prozent und bei Account Creation Attacks von 26 Prozent auf 32 Prozent.

Die Praxiserfahrung zeigt jedoch, dass Credential-Stuffing-Angriffe tatsächlich ein wesentlicher Angriffsweg sind, sodass es sinnvoll erscheint, die Relevanz der verschiedenen Angriffsformen in Unterweisungen für die verschiedenen Bereiche im Unternehmen bekannter zu machen.

Unternehmen sollten zudem eine Lösung für CIAM einsetzen, die vor Attacken wie Credential-Stuffing-Angriffen schützen kann, sicher und anwenderfreundlich.

Besser die Kundenbrille statt nur die IT-Brille bei CIAM-Projekten aufsetzen

Viele Unternehmen sehen die IT im Fokus ihrer CIAM-Projekte und versuchen, CIAM aus bestehenden IAM-Projekten heraus zu entwickeln. Wie die Umfrage zeigt, führt dies dazu, dass Kriterien, die für Kunden wichtig sind, leicht ins Hintertreffen geraten können. Dies muss und wird sich in Zukunft ändern.

Von Oliver Schonschek

Zweifellos sind Fragen der IT-Sicherheit und des Datenschutzes von zentraler Bedeutung, wenn digitale Angebote Erfolg bei Kunden haben sollen. Es ist deshalb gut und richtig, wenn 86 Prozent der Unternehmen die Absicherung ihrer Prozesse gegen Identitätsmissbrauch und Datendiebstahl für sehr wichtig halten. Können Kunden über das genutzte IAM-System zugreifen, steigt der Anteil der Unternehmen, die Datensicherheit als wichtig einstufen, noch weiter an und erreicht 93 Prozent.

Trotzdem ist es zu kurz gegriffen, wenn die Strategie zur Verwaltung der Kundenidentitäten und Berechtigungen bei weniger als 30 Prozent der befragten Unternehmen kundenbezogene Kriterien enthält, zwei Drittel der Unternehmen aber die Compliance und Sicherheitsfragen in den Mittelpunkt stellen.

Kundenerlebnis und Compliance schließen sich nicht aus

Gerade am Beispiel der Authentifizierungsverfahren zeigt sich, dass zum einen Kundenwünsche noch nicht genug im Bewusstsein der Unternehmensentscheider verankert sind: Moderne Verfahren der Authentifizierung wie Fingerprint-Reader haben nach Ansicht der Unternehmen weniger Zukunft als der Passwort-Klassiker, PINs oder Sicherheitsfragen. Die Kunden wollen aber gerade moderne Lösungen, die eine sichere Anmeldung komfortabel möglich machen.

Zum anderen setzen viele Unternehmen immer noch auf traditionelle Verfahren für den Zugangsschutz wie Benutzername und Passwort, die nicht nur bei Kunden eher unbeliebt sind, sondern die sich auch als zunehmendes Sicherheitsrisiko erwiesen haben.

Da Kunden versuchen, komplexe Passwörter, die man sich nur schwer merken kann, zu vermeiden, werden entweder Registrierungsprozesse abgebrochen, die starke Passwörter erzwingen wollen, oder die Kunden nutzen doch schwache Passwörter und setzen so ihre Daten einem Sicherheitsrisiko aus. Kommt es dann zu einem Datendiebstahl, leidet der Ruf des betroffenen Unternehmens darunter, erneut ein möglicher wirtschaftlicher Schaden, genau wie die abgebrochenen Registrierungsprozesse, die nichts anderes bedeuten als Kundenverlust.

CIAM Strategien brauchen unterschiedliche Perspektiven

Die Empfehlung lautet also, neben der IT immer auch die Kundenbereiche und die Entwicklung mit an den Tisch zu holen, wenn ein CIAM-Projekt geplant wird. Dadurch kann sichergestellt werden, dass auch neue Funktionen wie zum Beispiel eine biometrische Authentifizierung berücksichtigt werden, die sich die Kunden wünschen.

Da Online-Angebote, die Kundenwünsche nicht ausreichend berücksichtigen, auf Dauer keinen Erfolg haben, werden sich solche Online-Lösungen durchsetzen, die auch die Kundenbrille bei der Entwicklung genutzt haben und nicht nur die IT-Brille. Man sollte aber nicht auf den Druck des Marktes warten, sondern selbst die Brille wechseln, also neben der IT-Brille immer auch die Kundenbrille und Entwicklerbrille im CIAM-Projekt aufsetzen.

Interview

„Wir sind das Schweizer Taschenmesser auf dem CIAM-Markt“

Fragen an Vitor de Sousa, Area Vice President Sales, DACH & Eastern Europe, Auth0


Vitor de Sousa

Die Studie zeigt, nur 30 Prozent der befragten IT-Entscheider stellen den Kunden in den Fokus, wenn es um die CIAM-Strategie geht. Wie lässt sich das aus Ihrer Sicht ändern?

Der Kunde kommt deshalb zu kurz, weil zur Umsetzung einer wirksamen CIAM-Strategie sowohl die IT, die Security aber auch das Marketing und das Produktmanagement mitreden sollten. Nicht zu vergessen die Entwickler, die sich um die eigentliche Umsetzung kümmern. Die Ergebnisse machen allerdings deutlich, wie stark CIAM aus der Infrastruktur- und Sicherheitsecke betrachtet wird. Wird das kundenzentrierte Identitätsmanagement aus dieser Perspektive aufgezäumt, besteht die Gefahr, dass wertvolle Erkenntnisse zur Customer Experience, also dem Online-Kundenverhalten, außen vor bleiben. Mein Rat an die verantwortlichen Entscheider daher: Je stärker der Bereich des Managements von digitalen Kundenidentitäten wird, desto früher müssen technische und kundennahe Kompetenzen an einen Tisch.

Es zeigt sich, dass nicht wenige Kundendaten bereits in bestehenden IAM-Systemen verarbeitet werden. 61 Prozent der Kunden können zudem auf das System zugreifen. Warum braucht es dann überhaupt eine CIAM-Strategie?

Das kann man nicht so pauschal beantworten. Vielmehr sollte die Entscheidung für eine dezidierte CIAM-Strategie von den Anwendungsfällen abhängig gemacht werden. Denn IAM-Systeme können schnell an ihre Grenzen geraten, wenn sie bisher hauptsächlich für die Mitarbeiter-Authentifizierung mit fixen Anmeldevorgängen da waren. Für das Management von digitalen Kundenidentitäten, die über multiple Zugänge und Geräte auf ein Portal zugreifen, müssen die eingesetzten Systeme skalierbar und hochflexibel sein. Zudem werden direkt beim Login unterschiedliche Sicherheitsstufen benötigt, je nachdem wie sich der Online-Kunde registrieren und authentifizieren möchte. Hier geht es um das sichere und reibungslose Handling tausender Nutzerdaten. Unternehmen sollten daher die Art und Menge ihrer Authentifizierungsvorgänge genau analysieren, bevor sie eine CIAM-Strategie implementieren.

Können Sie das konkretisieren oder ein Beispiel geben?

Gern. Traditionelle IAM-Systeme werden häufig dazu genutzt, Mitarbeiterzugänge zu zentralisieren. Das hat den Vorteil, dass sie einfach und schnell zwischen unterschiedlichen Applikationen wechseln können, bringt aber auch meist den Wechsel von On-Premises zu Cloud mit sich. Auf dieser flexiblen und skalierfähigen Basis können dann ebenfalls digitale Kundendaten in beliebiger Größe verwaltet werden. Man muss aber auch die Perspektive des Endkunden einnehmen. Kommt man ihm in seinen Login-Gewohnheiten entgegen, kann das ein wesentlicher Faktor für die Gewinnung neuer Kunden sein. Diese Erfahrung haben wir bereits mit einigen Kunden im BtoC-Umfeld gemacht.

Wie kann Auth0 hier konkret unterstützen, zumal ein Großteil der Entscheider über Know-how-Mangel im Bereich IAM klagt?

Ich glaube, es gibt kein Unternehmen, dass groß genug wäre, es mit Identitätsmanagement in kompletter Eigenentwicklung aufzunehmen. Der entscheidende Punkt ist nicht die CIAM-Strategie an sich. Sondern vielmehr deren Umsetzung. Hier merken Unternehmen schnell, wie komplex Identitätsmanagement werden kann, und wie wenig Know-how sie dafür eigentlich verfügbar haben. Anfangs starten sie daher meist mit wenigen Funktionen, aber wenn dann die Zahl der Integrationspartner wächst, potenzieren sich auch Funktionen und Protokolle. Das alles bekommen sie dann nicht mehr in Eigenregie unter einen Hut. Wir als einer der spezialisiertesten Partner im Markt können hier mit hoher Entwickler-Expertise sowie individueller, cloudbasierter Integration für das komplette Identitätsmanagement punkten. Damit nehmen wir unseren Kunden die lästige Anwendungskomplexität ab. Man könnte sagen, wir sind das Schweizer Taschenmesser der CIAM-Anbieter.

Wie erklären Sie sich, dass Authentifizierungstechnologien für die IAM-Nutzer zu Treibern von CIAM werden, dann aber viele Entscheider weiterhin auf das gute alte Passwort setzen?

Vermutlich möchten Unternehmen auch in Zukunft nicht auf das gute alte Passwort verzichten, da es eine breite Akzeptanz bei den Nutzern hat. Viele von ihnen halten es immer noch für „gut genug“. Das liegt zu einem großen Teil daran, dass der Entwicklung und breitenwirksamen Vermarktung von einfachen und zugleich hochsicheren Identitätslösungen zu wenig Priorität eingeräumt wird. Wir müssen dringend dahinkommen, dass der Login beispielsweise in Form einer passwortlosen oder adaptiven Multifaktor-Authentifizierung als so einfach wahrgenommen wird, wie einen Lichtschalter zu betätigen. Mein Rat an die Entscheider daher: Je dominanter der Bedarf des Managements von digitalen Kundenidentitäten wird, desto eher müssen technische und kundennahe Kompetenzen an einen Tisch.

Auth0 Deutschland
eine Produkteinheit von Okta

https://auth0.com/de

Studiensteckbrief

Herausgeber	CIO, CSO und COMPUTERWOCHE
Exklusiver Studienpartner	Auth0
Grundgesamtheiten	Oberste (IT-)Verantwortliche von Unternehmen in der DACH-Region: strategische (IT-)Entscheider im C-Level-Bereich und den Fachbereichen (LoBs), IT-Entscheider & IT-Spezialisten aus dem IT-Bereich
Teilnehmergenerierung	Stichprobenziehung in der IT-Entscheider-Datenbank von IDG Business Media sowie zur Erfüllung von Quotenvorgaben über externe Online-Access-Panel; persönliche E-Mail-Einladungen zur Umfrage.
Gesamtstichprobe	288 abgeschlossene und qualifizierte Interviews
Untersuchungszeitraum	23. bis 29. September 2021
Methode	Online-Umfrage (CAWI)
Fragebogenentwicklung	IDG Research Services in Abstimmung mit dem Studienpartner Auth0
Durchführung	IDG Research Services

Stichprobenstatistik

Branchen*

Land- und Forstwirtschaft, Fischerei, Bergbau	8,0 %
Energie- und Wasserversorgung	10,4 %
Chemisch-pharmazeutische Industrie, Life Science	14,9 %
Medizin- und Labortechnik	8,3 %
Metallerzeugende und -verarbeitende Industrie	11,1 %
Maschinen- und Anlagenbau	12,8 %
Automobilindustrie und Zulieferer	6,6 %
Herstellung von elektrotechnischen Gütern, IT-Industrie	18,4 %
Konsumgüter-, Nahrungs- und Genussmittelindustrie	4,9 %
Medien, Papier- und Druckgewerbe	2,8 %
Baugewerbe, Handwerk	3,1 %
Groß- und Einzelhandel (inkl. Online-Handel)	12,2 %
Banken und Versicherungen	16,3 %
Transport, Logistik und Verkehr	9,0 %
Dienstleistungen für Unternehmen	13,5 %
Hotel- und Gastgewerbe, Tourismus	5,2 %
Öffentliche Verwaltung, Gebietskörperschaften, Sozialversicherung	6,3 %
Schule, Universität, Hochschule	3,1 %
Gesundheits- und Sozialwesen	2,8 %
Andere Branchengruppe	5,9 %

Unternehmensgröße deutschlandweit

Weniger als 100 Beschäftigte	1,4 %
100 bis 499 Beschäftigte	20,5 %
500 bis 999 Beschäftigte	36,5 %
1.000 bis 9.999 Beschäftigte	32,6 %
10.000 Beschäftigte und mehr	9,0 %

Umsatzklasse deutschlandweit

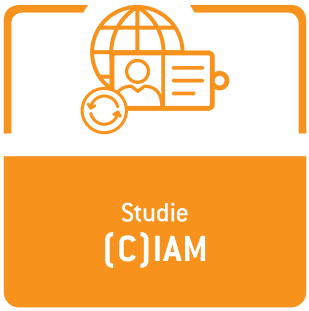
Weniger als 50 Millionen Euro	7,3 %
50 bis 99 Millionen Euro	21,9 %
100 bis 999 Millionen Euro	35,4 %
1 bis 2 Milliarden Euro	18,4 %
>2 bis 5 Milliarden Euro	13,2 %
>5 Milliarden Euro und mehr	3,8 %

Jährliche Aufwendungen in IT-Systeme

Weniger als 1 Million Euro	15,6 %
1 bis 10 Millionen Euro	47,2 %
>10 bis 100 Millionen Euro	31,6 %
>100 Millionen Euro und mehr	5,6 %

*** Mehrfachnennungen möglich**

IDG
RESEARCH SERVICES



auth0 okta