CIO

CSO
FROM IDG

VON IDG
COMPUTERWOCHE
VOICE OF DIGITAL

DIE WICHTIGSTEN ERGEBNISSE

präsentiert von

auth0 okta

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.

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.

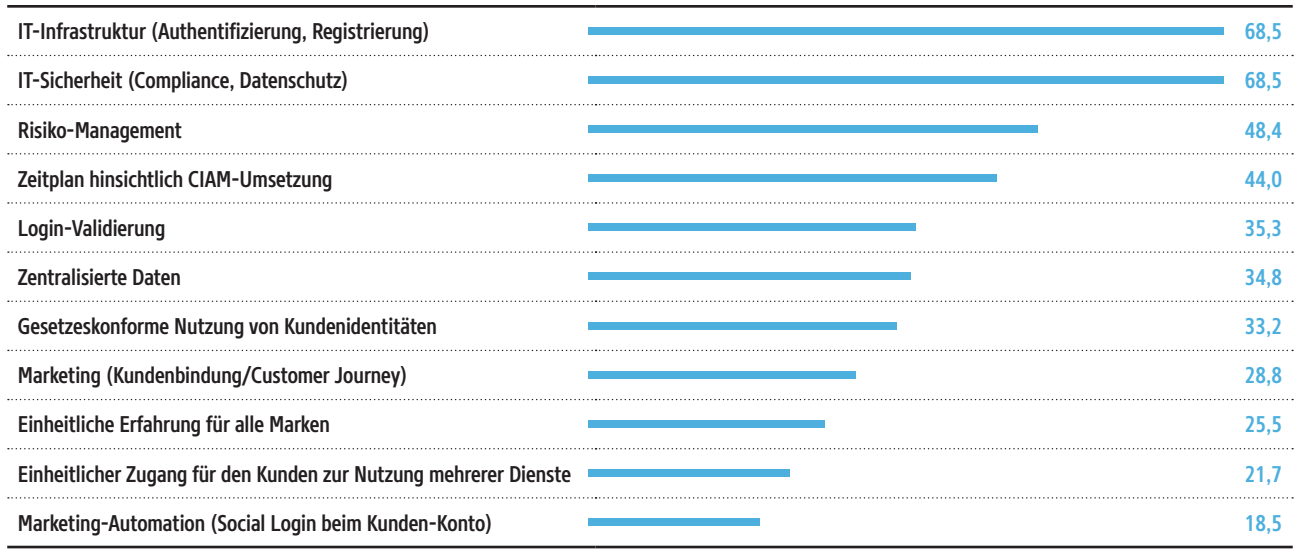
Anforderungen, die sich speziell auf Kundenbindung, Customer Journey, einheitliche Erfahrung für alle Marken, einheitlichen Zugang für den Kunden zur Nutzung mehrerer Dienste und auf Marketing-Automation beziehen, erreichen maximal 29 Prozent der Nennungen.

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

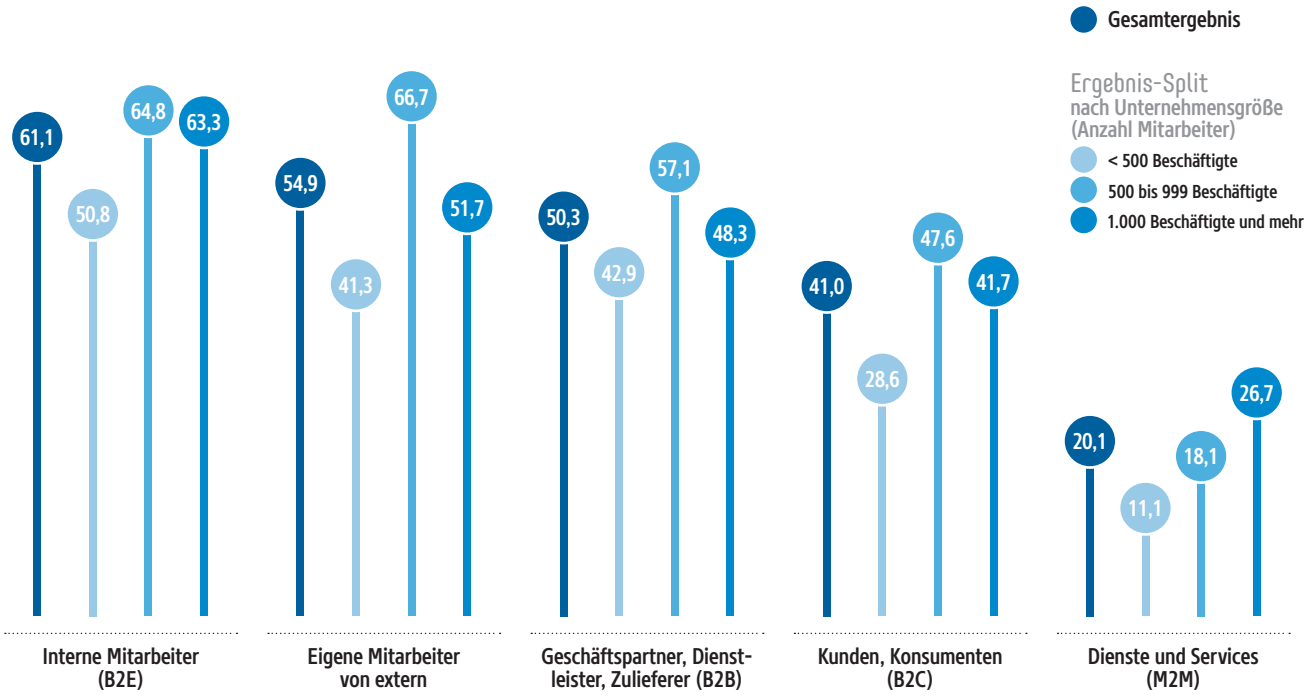


* Um den Anforderungen an eine valide Studie gerecht zu werden, wurden insgesamt 288 qualifizierte Interviews mit (IT-)Verantwortlichen in Unternehmen der DACH-Region aus allen Unternehmensbereichen (C-Level, IT, Fachbereiche) und aus allen Branchen durchgeführt.

2

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.

3

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.

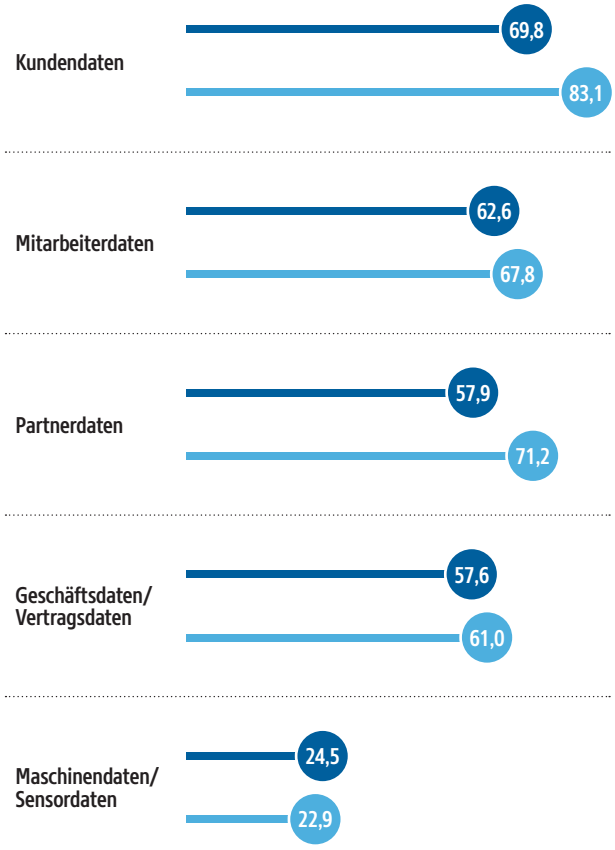
Kundendaten dominieren die Datenverarbeitung in IAM-Systemen, auch dann, wenn man nicht nur die Unternehmen betrachtet, die Kundenzugriffe auf ihr IAM erlauben.

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.

4 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.

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: < 10 Mio. Euro	10 Mio. Euro und mehr
IT	83,9	79,7	89,8
(IT-)Security	56,8	55,1	59,2
Produkt-Entwicklung (Forschung & Entwicklung)	44,1	49,3	36,7
Kundenservice	41,5	50,7	28,6
Vertrieb	37,3	37,7	36,7
Marketing	34,7	40,6	26,5
Rechtsabteilung	16,1	18,8	12,2
Andere Unternehmensbereiche	0,8	1,4	0,0

4

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.

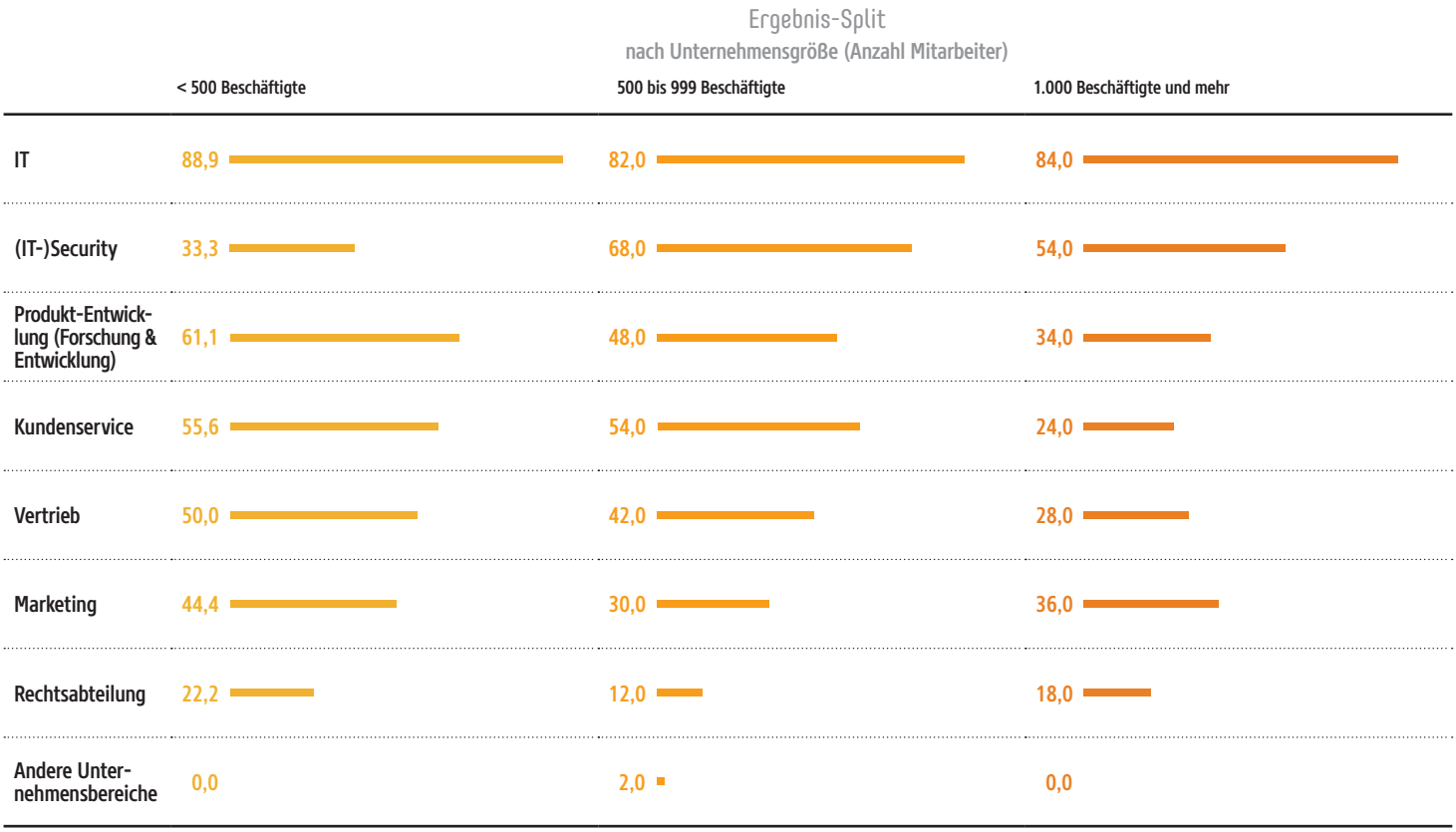
Die starke Gewichtung von IT und IT-Sicherheit als Entscheider in der CIAM-Strategie kann dazu führen, dass CIAM-Projekte aus einem bestehenden IAM-Projekt begonnen werden, da bei IAM die IT stark involviert ist. Klassische IAM-Lösungen würden dann für CIAM-Vorhaben eingesetzt, ohne jedoch die dafür 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.

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



Exklusiver Studienpartner

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

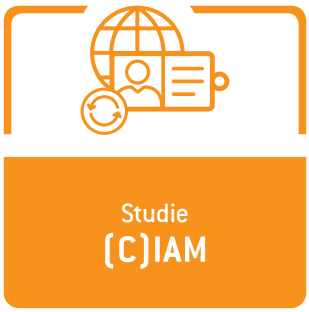
Hintergrund zu unserem Studienpartner

Auth0, eine Produkteinheit von Okta, verfolgt einen modernen Ansatz zum Thema Identitätsmanagement und ermöglicht es Organisationen, jedem Benutzer sicheren Zugang zu jeder Anwendung zu gewähren. Die Auth0-Plattform ist eine hochgradig anpassbare Plattform, die so einfach zu bedienen ist, wie Entwicklungsteams es sich wünschen und so flexibel, wie sie es benötigen. Auth0 sichert jeden Monat Milliarden von Login-Transaktionen und bietet Komfort, Datenschutz und Sicherheit, damit sich Kunden auf Innovationen konzentrieren können.
Weitere Informationen finden Sie unter https://auth0.com/de.

Was IAM und CIAM unterscheidet

	CIAM	IAM
Skalierbarkeit	CIAM-Systeme müssen hohe Datenströme bewältigen und für Millionen von Kunden skalieren.	IAM-Systeme müssen Datenströme für Hunderte Mitarbeiter skalieren.
Sicherheit	Die Kunden, die auf die Dienste zugreifen, sind den Unternehmen nicht bekannt. Der Schutz ihrer Daten kann nur über den Login funktionieren.	Die Mitarbeiter, die auf die Dienste zugreifen, sind den Unternehmen bekannt. Für den Schutz gibt es verschiedene Möglichkeiten, da sie sich über unterschiedliche Zugänge anmelden.
Verfügbarkeit	CIAM braucht einen Cloud-Service mit hoher Redundanz. Denn wenn Kunden der Zugang auf die Dienste nicht möglich ist oder Online-Portale ausfallen, verliert das Unternehmen Umsatz.	IAM-Systeme sollten ebenfalls in die Cloud verlagert werden. Wenn Mitarbeitende nicht auf digitale Dienste zugreifen können, schadet das der Arbeitgeberzufriedenheit sowie der Produktivität.
Flexibilität	Use Cases von Endkunden sind vielfältiger und erfordern daher je nach Szenario mehr Flexibilität. Denn Kunden können von jedem Gerät aus auf einen Dienst zugreifen und sie haben individuelle Anmeldemöglichkeiten, zum Beispiel mit Benutzername und Passwort oder Profile von Social Media. Diese müssen möglicherweise im Hintergrund verknüpft werden, damit die Nutzer auf einen zentralen Zugang zugreifen können.	Mitarbeitende nutzen in der Regel firmeneigene oder privat zugelassene Geräte auf Basis entsprechender Regeln. Sie brauchen jederzeit schnelle und sichere Authentifizierungsmöglichkeiten, um sich Zugang zu entsprechenden Apps zu verschaffen.

IDG
RESEARCH SERVICES



auth0

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