CIAM vs. IAM:

Warum herkömmliche IAM-Systeme nicht für Kunden verwendet werden sollten

Die Unterschiede zwischen CIAM und IAM

Das Schlagwort „Digitale Identität" steht im Mittelpunkt der digitalen Transformation eines jeden Unternehmens. Der Wert von Kundenprofildaten, die mit Kundenidentitäten verknüpft sind, ist enorm gestiegen und ist nun ein entscheidender Erfolgsfaktor für viele Unternehmen. Die digitale Identität bildet die Grundlage für die Analyse, das Verstehen und die Vorhersage des Verhaltens von Kunden und von Customer Journeys – vom Erstkontakt bis hin zu Kaufentscheidungen und langfristiger Markentreue.

Irrtümlicherweise wird oft geglaubt, dass die für das Customer Identity and Access Management (CIAM) erforderliche Technologie mit der für das herkömmliche Identity Access Management (IAM) identisch sei. Herkömmliche IAM-Lösungen, auch als Unternehmens-, Mitarbeiter- oder Belegschafts-IAM bezeichnet, sind die IT-Systeme, die dafür sorgen, dass nur die eigenen Mitarbeiter oder bekannte Geschäftspartner eines Unternehmens auf das Unternehmensnetzwerk und dessen Ressourcen zugreifen können.

Herkömmliche IAM-Lösungen sind in der Regel gut bewährte Systeme, weswegen einige Unternehmen die folgende falsche Annahme treffen: „Da wir diese Technologie bereits intern haben, kann es doch nicht so schwierig sein, diese auf unsere Kunden auszuweiten." Dieser Ansatz basiert auf einer erheblichen Unterschätzung der Unterschiede zwischen IAM-Systemen für Belegschaften und solchen für Kunden. Auch die Komplexität, was das Verwalten von Kundenidentitäten für die öffentlichen Digital Properties eines Unternehmens betrifft, wird dabei gern unterschätzt. Für das CIAM gelten grundverschiedene – und weitaus anspruchsvollere – Anforderungen als für das IAM für Belegschaften. Daher kann es problematisch werden, wenn IAM-Lösungen für Belegschaften einfach umfunktioniert werden.

Ein herkömmliches IAM kann keine Einblicke in die Identität von Nutzern, in die von ihnen durchgeführten Aktivitäten und in die Aspekte, die deren digitales Verhalten beeinflussen, geben.

Das Umfunktionieren des herkömmlichen IAM zu CIAM ist keine geeignete Lösung

Da das herkömmliche IAM Mitarbeitern den Zugriff auf interne Systeme erleichtern soll, kann es keine Einblicke in die Identität eines Nutzers bieten. Im Gegenteil, es wird eine Identität angenommen, und erweiterte Daten (wie die Aktionen, die ein Nutzer durchführt, und Aspekte, die seine „Reise" und sein Verhalten innerhalb der digitalen Welt beeinflussen) können nicht nachverfolgt werden. Doch Unternehmen benötigen diese Art von Einblicken in Daten, um ihre Kunden zu verstehen und im digitalen Marktsegment wettbewerbsfähig zu sein.

Ein weiterer Unterschied: In vielen der größten Unternehmen müssen im Rahmen des herkömmlichen IAM ggf. bis zu zehntausende Mitarbeiteridentitäten verwaltet werden. Bei Marken mit hohen Volumina müssen hingegen Kundenkonten im zwei-, wenn nicht gar dreistelligen *Millionenbereich* gleichzeitig verarbeitet werden. Noch dazu erwarten moderne Verbraucher einen reibungslosen Ablauf. Eine Identitätslösung muss Skalierungsmöglichkeiten bieten, um diesen Workload mit kaum oder gar keiner wahrnehmbaren Latenz zu erfüllen.

Ein träges Identitätsmanagement-System wirkt sich kontraproduktiv auf gezielte und hart umkämpfte Geschäftsbemühungen aus.

Eine kürzlich von Akamai durchgeführte Studie hat ergeben, dass eine Verzögerung von zwei Sekunden beim Laden von Webseiten die Absprungrate um 103 % erhöht, und 53 % der Besucher mobiler Websites verlassen eine Seite, wenn diese länger als drei Sekunden lädt.[1] Wenn Ihr Identitätsmanagement-System also ausfällt oder sich aufgrund der Auslastung verlangsamt, werden sehr wahrscheinlich Ihre Konversionsraten und Ihr Umsatz ebenfalls in Mitleidenschaft gezogen. Ironischerweise sind Auslastungsspitzen und erhöhter Kundentraffic in der Regel die Früchte erfolgreicher Kampagnen. Somit wirkt sich ein träges Identitätsmanagement-System kontraproduktiv auf gezielte und hart umkämpfte Geschäftsbemühungen aus.

Dedizierte CIAM-Plattformen wie die Akamai Identity Cloud sind so konzipiert, dass sie Unternehmen einen maximalen Nutzen aus Kundenprofildaten bieten. Solche Lösungen ermöglichen ein nahtloses und reibungsloses Kundenerlebnis, sodass Aufgaben wie Anmeldung, Authentifizierung oder die Verwaltung von Nutzereinstellungen die Aktivität nicht behindern. Darüber hinaus sorgen CIAM-Technologien für den entscheidenden Schutz personenbezogener Daten in öffentlichen Netzwerken. Ferner ermöglichen sie globalen Unternehmen, die vielfältigen und sich häufig ändernden Datenschutzbestimmungen zuverlässig einzuhalten.

In der folgenden Tabelle sind die wichtigsten Unterschiede zwischen herkömmlichem IAMund CIAM sowie ihren Anwendungen aufgeführt.

Herkömmliches IAM	CIAM
Verwaltung von **Mitarbeiteridentitäten** innerhalb eines Unternehmens.	Verwaltung von **Kundenidentitäten** auf digitalen, an Kunden gerichteten, mehrkanaligen Websites (Web, Mobile, IoT).
Nutzer **werden von ihrem Unternehmen registriert.** Dabei werden wichtige Profildaten von der Personal- oder IT-Abteilung eingetragen.	Nutzer **registrieren sich selbst** und generieren ihre eigenen nutzerspezifischen Daten.
Authentifizierung gegen interne **Directory-Dienste.**	Authentifizierung gegen **öffentliche Dienste** wie OpenID und soziale Medien sowie Directory-Dienste und externe Dienste zur Überprüfung von Anmeldedaten.
Nutzer sind bekannt und (an das Unternehmen) gebunden: Mitarbeiter, Auftragnehmer, Partner. **Die Identität kann angenommen werden.**	Nutzer sind **unbekannt** (bis zur Registrierung) und können mehrere und gefälschte Konten erstellen. **Die Identität kann nicht angenommen werden.**
Nutzer der Belegschaft sind Latenzzeiten und schlechter Performance gegenüber **toleranter**, da sie häufig **keine Alternative haben.**	Kunden und Interessenten haben **eine sehr geringe Toleranz** gegenüber schlechter Performance, weil sie **viele attraktive Alternativen** haben.
Skalierbar von **zehn- auf hunderttausende Nutzer,** mit jeweils einer Identität.	Skalierbar auf bis zu **hunderte Millionen von Nutzern**, mit Kundenidentitäten im Milliardenbereich.
Der herkömmliche Identity Provider (IdP) ist in der Regel **ein zentrales internes IT-System.**	**Viele dezentrale Identity Provider:** Social Login über Facebook, Google, LinkedIn usw. sowie herkömmliche Anmeldung.
Viele heterogene IT-Systeme in einem **geschlossenen Unternehmensnetzwerk.**	Viele heterogene IT-Systeme **in öffentlichen Netzwerken (Internet).**
Profildaten von Mitarbeitern werden für **administrative und betriebliche Zwecke erfasst.**	Profildaten von Kunden werden für **äußerst kritische Geschäftszwecke** (Transaktionen, Marketing, Personalisierung, Analyse und Business Intelligence) erfasst.
Integration in **HR- und ERP-Systeme.**	Integration in **eine breite Palette an Technologien für Marketing- und Vertriebsautomatisierung**, **Analysesysteme** sowie **Sicherheits- und Compliance**-Lösungen.
Die Verwaltung personenbezogener Daten sowie der Privatsphäre/Einstellungen/Einwilligung der Nutzer erfolgt ausschließlich in einer streng **kontrollierten, homogenen Unternehmensumgebung.**	Der Umgang mit personenbezogenen Daten unterliegt einer **Vielzahl von Privatsphären- und Datenschutzvorschriften**, wobei die Nutzer Einstellungen zu Präferenzen und Einwilligungen anzeigen, ändern und widerrufen können müssen.

Lesen Sie „Entwicklung oder Kauf? Ein Leitfaden für Customer Identity and Access Management“, um mehr über CIAM-Lösungen zu erfahren. Oder besuchen Sie akamai.com/identitycloud, um mehr darüber zu erfahren, wie Sie mit CIAM von Akamai vertrauenswürdige digitale Erlebnisse für Ihre Endnutzer bereitstellen können.

QUELLE

1) https://www.akamai.com/de/de/about/news/press/2017-press/akamai-releases-spring-2017-state-of-online-retail-performance-report.jsp

Akamai

Als weltweit größte und renommierteste Plattform für die Cloudbereitstellung unterstützt Akamai seine Kunden dabei, ein optimales und sicheres digitales Erlebnis bereitzustellen – auf jedem Gerät, an jedem Ort und zu jeder Zeit. Die stark verteilte Plattform von Akamai weist eine beispiellose Skalierbarkeit auf und bietet Kunden somit eine überragende Performance sowie einen umfassenden Bedrohungsschutz. Das Akamai-Portfolio für Website- und App-Performance, Cloudsicherheit sowie Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice und Rund-um-die-Uhr-Überwachung begleitet. Warum führende Finanzinstitute, Onlinehändler, Medien- und Unterhaltungsanbieter sowie Behörden auf Akamai vertrauen, erfahren Sie unter www.akamai.de, im Blog blogs.akamai.com/de oder auf Twitter unter @AkamaiDACH oder @Akamai. Veröffentlicht: April 2019