cidaas

Leitfaden: Customer Identity und Access Management

Was gilt es bei der Wahl einer CIAM-Lösung zu beachten?

Whitepaper

Der Digitalisierungseffekt
Die Welt im Umbruch

Über den Autor

Sadrick Widmann ist Chief Product Officer von cidaas, dem ersten komplett in Deutschland entwickelten und gehosteten Customer Identity und Access Management. Er kennt und versteht die Anforderungen, die mit einer digitalisierten Welt einhergehen und hilft Kunden beim Aufbau von identitätsbasierten Geschäftsmodellen.

PROLOG

Mit der Digitalisierung verändern sich die klassischen Geschäftsmodelle. Die Geschwindigkeit, mit der neue Technologien auf den Markt gebracht werden, nimmt von Tag zu Tag zu und verändert unser privates wie auch unser berufliches Leben. Neue Geschäftsmodelle sind entstanden, die zunehmend data-driven und cloud-fähig, aber vor allem kundenzentriert sind. Was bei einer solchen kundenorientierten strategischen Geschäftstransformation eine grundlegende Rolle spielt, sind die Identitäten der involvierten Personen.

>Die Verwaltung von Identitäten wird zum Erfolgsfaktor

In einem vollständig vernetzten, digitalen Ökosystem stellt die Verwaltung einer schier unbegrenzten Zahl an Benutzeridentitäten, seien es Mitarbeiter- oder Kundenidentitäten, eine Herausforderung dar. Auf den Konsumenten bezogen wird das Kundenerlebnis zum kritischen Erfolgsfaktor, um im steigenden Wettbewerb bestehen zu können. Jeder Interaktionspunkt muss ein konsistentes Erlebnis darstellen, gleichzeitig aber auch die sensiblen Daten der Verbraucher schützen und den Datenschutzvorgaben der EU-DSGVO entsprechen. Nicht nur im Business-to-Consumer (B2C) Umfeld hängt die Wettbewerbsfähigkeit stark von der Bereitstellung des richtigen Kundenerlebnisses ab, auch im Business-to-Business (B2B) Bereich etabliert sich dieser Ansatz zunehmend.
Der IT-Markt hat reagiert und Lösungen für das Identitätsmanagement auf den Markt gebracht, die leicht in bestehenden IT-Infrastrukturen integriert werden können. Dabei gilt es zwei Ausprägungen zu unterscheiden: internes und externes Identity und Access Management (IAM), wobei letzteres als Customer Identity und Access Management (CIAM) tituliert wird.

>Ein Customer Identity und Access Managment rüstet Unternehmensprozesse für die digitale Zukunft

Doch worin besteht der genaue Unterschied zwischen IAM und CIAM? Und welche Unternehmen profitieren davon? Dieser Leitfaden gibt Ihnen einen Überblick über die Unterschiede und die wichtigsten Funktionen, auf die Sie bei der Auswahl einer CIAM-Lösung achten sollten.
Eines können wir jedoch gleich vorwegnehmen: ein effektiv eingesetztes Customer Identity und Access Management System ist längst zu einem Must-Have in der Digitalisierungsstrategie eines jeden Unternehmens, unabhängig von dessen Branche und Größe, geworden.

Ich wünsche Ihnen eine spannende Lektüre mit interessanten Einblicken
Ihr Sadrick Widmann

INHALT

CUSTOMER IDENTITY UND ACCESS MANAGEMENT

Generell

> Traditionelles IAM

Klassisches Identity and Access Management, kurz **IAM**, ist ein System zur Authentifizierung und Autorisierung aller Personen innerhalb eines Unternehmens.

Hauptaufgabe ist , die Identitäten, Rollen und Berechtigungen der verbundenen Akteure zu verwalten. Mitarbeiter, Freelancer, Partner und alle weiteren Stakeholder, die mit dem Unternehmen verbunden sind, erhalten die für sie korrekten Zugriffsrechte auf alle digitalen Ressourcen eines Unternehmens.

Gemäß dem „Need to Know-Prinzip" hat jeder genau die Zugriffe und Berechtigungen, die seiner Rolle im Unternehmen entsprechen.

Dieser Ansatz ist effektiv, solange es sich um die Verwaltung einer definierten Anzahl von Benutzern handelt. Durch den Digitalisierungseffekt und die damit verbundene Vernetzung wird heute jedoch mehr und mehr verlangt, dass auch externe Stakeholder, wie Kunden, Lieferanten, Partner und sogar „Dinge" eigene Identitäten bekommen, um auf Apps, Services und Daten zugreifen zu können. Beispielsweise ist es heute üblich, dass ein Kunde oder auch ein Lieferant seine persönlichen Daten im Kundenkonto selbst verwalten kann.

> Der Ansatz eines klassischen IAM

Konventionelle Identity und Access Management Lösungen (IAM) werden mit den folgenden Zielsetzungen entwickelt:

- Überprüfung der Identitäten einer bekannten Gruppe von Benutzern
- Vermeidung von Datenschutzverletzungen durch kontrollierten Zugriff

Um den Zugriff auf sensible Daten auch außerhalb von Unternehmensgrenzen verfügbar zu machen, hat sich neben dem internen Identitätsmanagement daher auch ein externes herauskristallisiert, welches allgemein unter Customer Identity und Access Management (CIAM) bekannt ist.

CIAM vs. IAM
Das sind die Unterschiede

> CIAM als Weiterentwicklung des klassischen IAM

CIAM verändert und erweitert den traditionellen IAM Gedanken. Nach wie vor technisch geprägt, umfasst modernes Identity und Access Management Aspekte wie Registrierungsprozesse sowie das Sammeln und Verwenden von Daten. Somit bildet es auch die Schnittstelle zu Marketing Services, um den Kunden mit zielgerichteten Informationen zu versorgen.

CIAM-Lösungen werden mit dem Schwerpunkt auf **Kundenzufriedenheit, Skalierbarkeit und Anpassungsfähigkeit** an sich ständig ändernde Markttrends und zunehmende Sicherheitsanforderungen durch steigende Cyberkriminalität, entwickelt.

Dazu bedarf es **flexiblen Workflows, umfangreichen Authentifizierungsverfahren, hoher Skalierbarkeit,** aber auch **standardisierten Prozessen**, um die wachsenden gesetzlichen und regulatorischen Vorgaben zu erfüllen.

> CIAM schafft einen 360° Blick auf Benutzerdaten

Damit eine CIAM-Lösung eine Rundum-Sicht auf Identitäten schafft und gleichzeitig die Balance zwischen Marketing, Sicherheitsanforderungen und regulatorischen Compliance-Richtlinien hält, sollte eine Lösung out-of-the-box folgende Aspekte beinhalten:

- **Zugriffssicherheit durch moderne Authentifizierungsverfahren:**
  die Bereitstellung sensibler Daten muss jederzeit abgesichert sein. Moderne Authentifizierungsverfahren mit biometrischen Faktoren wie Fingerabdruck, Gesichtsscan, etc. sollten vorhanden sein.

- **Compliance:**
  EU-DSGVO-konforme Einwilligungsverwaltung zur Einhaltung der Datenschutzvorgaben.

- **Skalierbarkeit:**
  Nutzerzahlen können schnell, immens steigen – das sollte ein CIAM verkraften können.

CIAM vs. IAM
Das sind die Unterschiede

- **Integration:**
  nahtlose und einfache Integration in bestehende Softwarelandschaft.

- **Benutzer-Self-Services:**
  einfache Aktionen wie z.B. die erste Registrierung oder das Ändern von Passwörtern sollte den Nutzern selbst überlassen sein.

- **Social Login und Single-Sign-On (SSO):**
  einfache und bequeme Anmeldeprozesse ermöglicht die Nutzung eines Social Login über gängige Social Media Provider. Der Benutzer loggt sich mit seinem bekannten Nutzerprofil ein. Über die Funktion Single Sign-On (SSO) bekommt er Zugriff auf alle digitalen Services des Unternehmens und muss sich nicht mehrmals anmelden.

- **Standards statt Customizing:**
  Wählen Sie eine Lösung, die auf Standards wie OAuth2 oder OpenID Connect setzt. Da viele heterogene Systeme miteinander verbunden werden müssen, ist eine genormte Vorgehensweise und keine Eigenentwicklung empfehlenswert.

- **Marketingfunktionalitäten:**
  sorgen für einen direkten und individuellen Dialog mit dem Kunden.

Die Auswahl einer Softwarelösung für das Customer Identity und Access Management ist jedoch erst nach einer genauen Analyse der eigenen Geschäftsprozesse sinnvoll.

DIE GRETCHENFRAGE

Make or Buy

Vor allem, wenn ein Unternehmen über eine eigene IT-Abteilung verfügt, stellt sich oftmals die Frage, welche Services von der eigenen Mannschaft entwickelt werden können und welche zugekauft werden sollten. Im Zuge der Digitalisierung nimmt das alte Thema „make or buy" wieder neue Fahrt auf.

Als Unternehmen sollte man sich jedoch die Frage stellen, ob sich bei der Entwicklung einer hausinternen Lösung klare Wettbewerbsvorteile ergeben. Besonders wenn Unternehmen bereits ein IAM-System im Einsatz haben, erscheint ein Aufsetzen weiterer Funktionalitäten auf diese Basis verlockend. Auf den ersten Blick erscheinen interne Entwicklungen oftmals einfach, am Ende stellt sich aber meist heraus, dass eigengestrickte Lösungen mehr Zeit und Geld kosten und auch nicht so effektiv sind, wie standardisierte Lösungen. Wenn es um Identitätsmanagement geht, das auch immer eng mit hochsensiblen Daten verbunden ist, gilt es besonderen Augenmerk auf die Aspekte **Sicherheit, Datenschutz und Authentifizierung** und der damit einhergehenden Anforderungen zu legen. Hier empfiehlt es sich, auf Experten zu vertrauen.

> Für den Einsatz einer standardisierten CIAM-Lösung sprechen die folgenden Punkte:

- **geringere Kosten:**
  die Implementierung einer Standard CIAM-Software ist unkompliziert und die Aktivierung der einzelnen Funktionen in Kürze umgesetzt. Eine gute CIAM-Lösung liefert immer fertige Software Development Kits (SDK) mit, sodass sich Ihr Team auf die Konfiguration der Lösung konzentrieren kann und nicht auf dessen Programmierung.

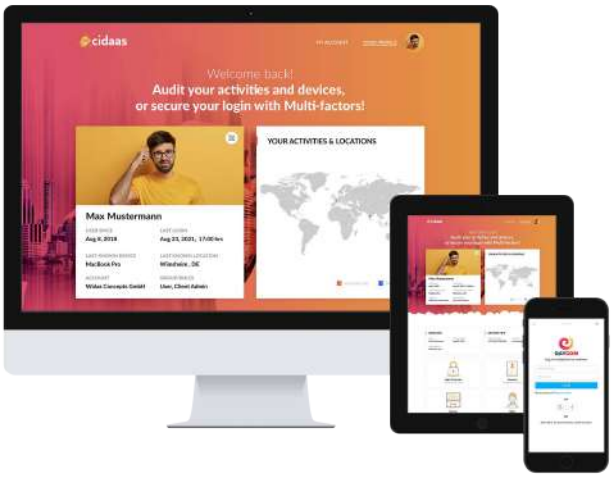
- **Höchste Sicherheit für sensible Daten:**
  mit einem CIAM werden hochsensible Daten verwaltet, die vor unbefugten Zugriffen geschützt werden müssen. Bei Verwendung einer Standardlösung liegt es in der Verantwortung des Anbieters, dass stets die aktuellsten Sicherheitsrichtlinien und Zertifikate verwendet werden und auf Standards wie OAuth2, SAML, etc. gesetzt wird.

DIE GRETCHENFRAGE
Make or Buy

- **Hohe Akzeptanz bei den Benutzern:**
  Standard CIAM-Lösungen verwenden die gängigsten und benutzerfreundlichsten Login- und Authentifizierungsmethoden und finden so eine hohe Akzeptanz bei den Benutzern.

- **Skalierbarkeit:**
  Ihr Geschäft ist nicht statisch – Benutzerzahlen können schnell immens ansteigen. Beim Einsatz einer externen CIAM-Lösung müssen Sie die Kapazitäten nicht selbst freihalten, sondern überlassen dies dem Anbieter.

- **Support von Experten:**
  Die meisten Anbieter stellen ihren Kunden einen 24/7 Support zur Verfügung. Das Handling von Fragestellungen oder Störfällen liegt somit nicht in der Hand des eigenen Unternehmens, sondern kann nach extern ausgelagert werden. Was wiederum den eigenen Help-Desk, sofern überhaupt vorhanden, entlastet



Die Vorteile eines bestehenden, ausgereiften Identity Management System überwiegen meist gegenüber einer Eigenentwicklung.

Was gilt es bei der Wahl einer CIAM-Lösung zu beachten?

> CIAM ist nicht gleich CIAM

Der CIAM-Markt ist in den letzten Jahren stark gewachsen und mittlerweile sehr vielschichtig geworden. Hier das richtige Angebot zu finden, ist nicht immer einfach. Denn eines ist klar: **CIAM ist nicht gleich CIAM**. Es zeigen sich viele Unterschiede hinsichtlich einzelner Funktionalitäten sowie in den eingesetzten Technologien. Speziell die Themen **Multi-Faktor-Authentifizierung (MFA)** und **Single Sign-On (SSO)** beherbergen noch viel Wachstumspotential. Da jedes Produkt seine eigenen Schwerpunkte setzt und mit unterschiedlichsten Funktionssets einhergeht, gilt es die „Must-Haves" und die „Nice-to-haves" für die eigenen Unternehmensprozesse herauszukristallisieren.

Im folgenden Abschnitt stellen wir Ihnen die Funktionalitäten dar, die bei einem CIAM-System zwingend notwendig sind, um Ihr Unternehmen in der digitalen Zukunft voranzubringen.

Onboarding und Authentifizierung von Benutzern

Das Hauptziel eines Customer Identity und Access Management Systems ist, eine einheitliche digitale Identität zu schaffen, um eine konsistente, personalisierte Benutzererfahrung über alle Kanäle hinweg bereitzustellen. Um dieses Ziel zu erreichen, sollten die Anmelde- und Authentifizierungsprozesse für den Benutzer so komfortabel und bequem wie möglich gestaltet sein.

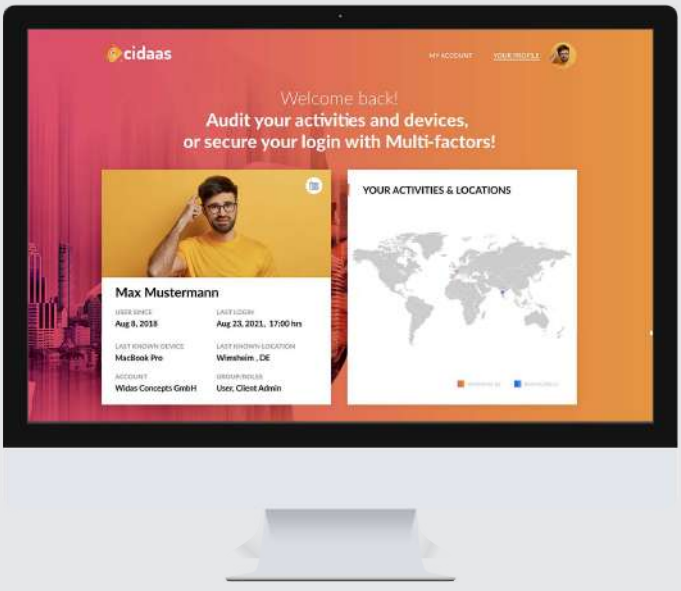
> Passwortloses Login / Social Login für die Anmeldung der Benutzer

Eine gute CIAM-Lösung sollte die Anmeldung über alle gängigen Identity Provider unterstützen. Im geschäftlichen Umfeld sind Office 365 oder Active Directory und im Consumer-Umfeld alle gängigen Social Media Plattformen (Facebook, Google,...) zu nennen. Die passwortlose Authentifizierung kann mit biometrischen Faktoren wie Touch ID, Sprache, Gesicht oder mit herkömmlichen Methoden wie E-Mail, SMS oder FIDO-basierten Verifikationen durchgeführt werden.

> moderne Multi-Faktor-Authentifizierungsmethoden

Der Einsatz eines zweiten Authentifizierungsfaktors soll sicherstellen, dass der wirkliche Inhaber des Accounts eine Aktion ausgelöst hat. Die Abfrage eines zweiten Faktors kann entweder bei jedem Login erforderlich sein, oder er wird nur dann abgefragt, wenn ein auffälliges Verhalten festgestellt wird und man davon ausgeht, dass nicht der tatsächliche Besitzer des Accounts die gewünschte Aktion ausgelöst hat. Diese Auffälligkeiten werden vom CIAM-System durch ein verhaltensbasiertes Clustering wie z.B. Standortdaten oder übliche Gerätenutzung erkannt. Die sicherste Variante der Multi-Faktor-Authentifizierung ist die Nutzung von biometrischen Merkmalen (Fingerabdruck, Gesichtsscan,...) zur Identifizierung einer Person.

Authentifizierungsverfahren - auf die Auswahl kommt es an



cidaas bietet eine Vielzahl an modernen, passwortlosen Loginmöglichkeiten und sorgt für eine sichere Authentifizierung.

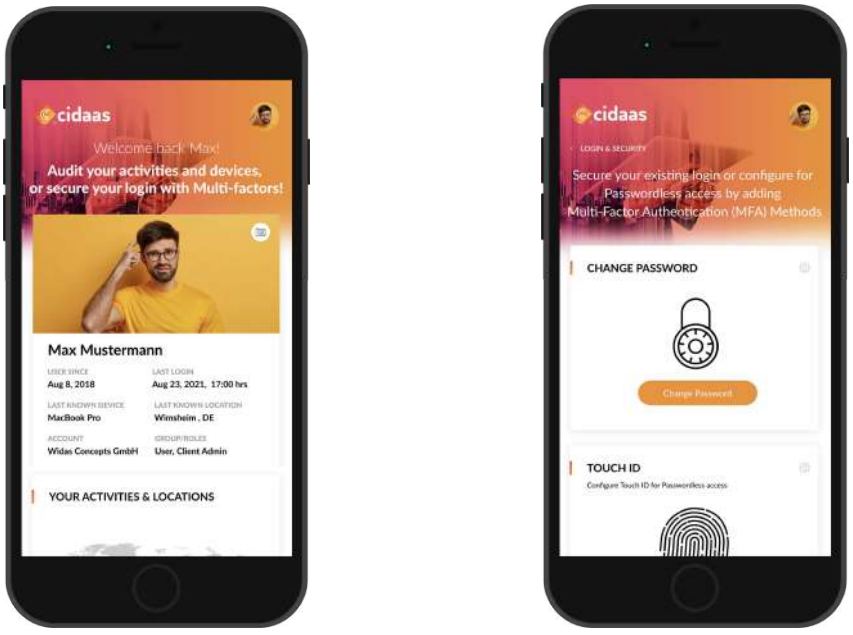
Jetzt entdecken

> Single Sign-On über alle Unternehmenskanäle

Single Sign-on, kurz SSO, sorgt für ein durchgängiges Anmeldeerlebnis. Der Kunde loggt sich einmal ein und kann dann alle digitalen Kanäle des Anbieters ohne nochmalige Anmeldung nutzen.

> User-Self Services für die Kontenverwaltung

Durch Benutzer-Self-Services können Kunden ihre hinterlegten Daten selbst verwalten, aktualisieren oder löschen.



Datenschutz und Sicherheit

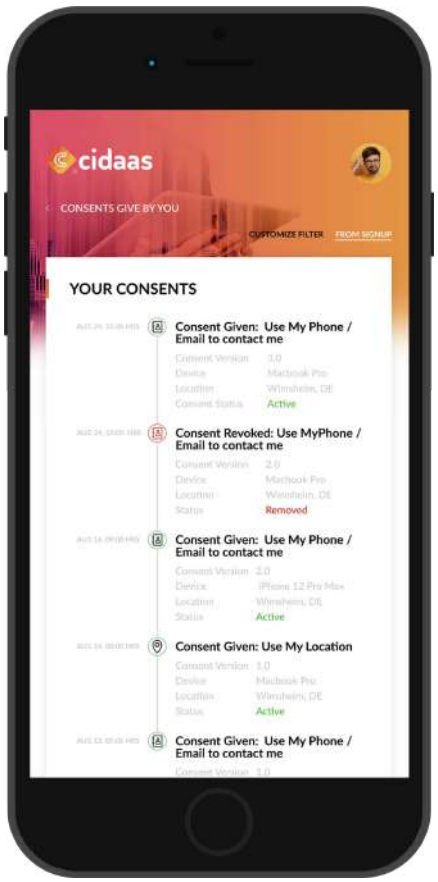
Zunehmende Cyberkriminalität und erhöhte Datenschutzanforderungen haben das Thema Sicherheit zur obersten Priorität werden lassen. Das digitale Unternehmen von heute tut daher gut daran, eine zentrale Zugriffsebene für sämtliche Daten zu schaffen.

> Einhalten von regionalen, branchenspezifischen oder betrieblichen Datenschutzbestimmungen

Ein CIAM hilft die vielfältigen Datenschutzbestimmungen umzusetzen und stellt die technischen Voraussetzungen bereit, um Einwilligungen und Datennutzungsbestimmungen zentral, an einem Ort, zu verwalten. Egal ob EU-DSGVO oder interne Compliance-Anforderungen – ein CIAM liefert das Handwerkszeug.

> Umgang mit personenbezogenen Daten

Die Bestimmungen der EU-DSGVO verlangen, dass personenbezogene Daten (personally identifiable information, PII) jederzeit eingesehen und bearbeitet werden können. Wenn Aktualisierungen oder Änderungen z.B. Weitergabe der Daten an Dritte notwendig sind, dann muss der Kunde aktiv aufgefordert werden, dies zu bestätigen. Darüber hinaus ist dafür Sorge zu tragen, dass dem Benutzer seine persönlichen Daten auf Wunsch bereitgestellt werden oder auch vollständig gelöscht werden können. Bei Nutzung eines CIAM haben die Benutzer selbst die volle Kontrolle über ihre sensiblen, personenbezogenen Daten und können Einwilligungen jederzeit einsehen und widerrufen. Auf Knopfdruck können alle zu diesem Zeitpunkt hinterlegten Daten bereitgestellt werden.



> Absicherung der Identitäten

Die Absicherung von Identitäten ist ein wesentlicher Bestandteil eines CIAM-Systems.
Dies wird unter anderem durch sichere Datenverschlüsselung sowie das Auslösen einer Zwei-Faktor-Authentifizierung bei verdächtigen Aktivitäten gewährleistet.

> verwendete Identitätsstandards

Bei der Evaluierung eines Identity Systems sollte darauf geachtet werden, dass auf Standardprotokolle wie OAuth2 oder OpenID Connect zur Authentifizierung und Autorisierung gesetzt wird.

Skalierbarkeit und Integration

Da IT-Infrastrukturen heute in den meisten Fällen sehr heterogen aufgestellt sind, sollte die Integration einer weiteren Softwarekomponente ohne aufwendige Programmierungen möglich sein. Weiterhin spielt in der heutigen Zeit, in der vorwiegend auf den Absatz digitaler Mehrwertdienste gesetzt wird, die Skalierbarkeit eine wichtige Rolle.

> Anbindung an bestehende IT-Systeme

Egal, wie die derzeitige IT-Landschaft betrieben wird: eine CIAM-Lösung sollte immer offene APIs zur Verfügung stellen, um eine einfache technische Integration der Identity-Lösung in die bestehende Business-Software zu gewährleisten. Oftmals stehen auch vorgefertigte SDKs (Software Development Kits) zur Verfügung, durch die man schnell alle vorhandenen Anwendungen anbinden kann.

> Erwartete Nutzerbasis

Das Wachstum von Organisationen ist oft schwer vorhersehbar. Bereits bei der Auswahl eines CIAM-Providers sollte darauf geachtet werden, dass der Service bei starker Nutzung gut performed und so skaliert werden kann, dass eine nahezu unbegrenzte Anzahl an Benutzern unterstützt wird.

cidaas - Customer Identity as a Service

> die erste komplett in Deutschland entwickelte und gehostete Lösung für ein effizientes Customer Identity und Access Management

Wie die vorangegangenen Kapitel gezeigt haben, spielen bei der Auswahl einer Identitätsmanagement-Lösung viele Faktoren eine wichtige Rolle.

Die Widas Unternehmensgruppe mit Sitz in Wimsheim bietet seit 1997 „Software made in Germany" und hat mit dem Cloud-Service **cidaas** ein **hochskalierbares und nahtlos integrierbares Customer Identity und Access Management** entwickelt. Basierend auf den Standards OpenID Connect und OAuth2 sorgt cidaas für **höchste Sicherheit bei der Schnittstellen-Authentifizierung**. Der Cloud-Service ist in Deutschland entwickelt und gehostet und wurde mit dem Gütesiegel „Software hosted in Germany" ausgezeichnet. Zur eindeutigen Prüfung der Benutzeridentitäten werden **starke Multi-Faktor-Authentifizierungsmethoden (MFA)** unter anderem auch durch biometrische Abfragen (Fingerabdruck, Gesichtsscan,...) genutzt.

KURZ UND KNAPP
CIDAAS - CUSTOMER IDENTITY

cidaas beinhaltet out-of-the-box einen umfassenden Funktionsumfang, der unter anderem die folgenden Features beinhaltet:

- Multi-Faktor-Authentifizierung
- Social Login
- Single Sign-On
- Höchste Zugriffssicherheit durch integrierte Betrugs- und Verdachtsfallerkennung
- Data Governance durch EU DSGVO-konformes Einwilligungsmanagement
- Absicherung Ihrer Portale und Web-APIs durch die Standards OAuth2 und OpenID Connect
- Benutzer Self-Services
- Gruppenmanagement (B2B Modul) für die einfache Rollen- und Rechteverwaltung Ihrer Geschäftspartner
- Stufenlose Skalierbarkeit entsprechend Ihren Anforderungen
- Modular aufgebaute Microservices Architektur sorgt für höchste Agilität
- Verschiedene Servicepakete je nach individueller Anforderung
- 24/7 Experten Support

cidaas bietet **Flexibilität, Skalierbarkeit, Sicherheit und Transparenz** und lässt sich nahtlos in jede bestehende Softwarelandschaft integrieren. Die Cloud-Software steht in 5 Service-Paketen zur Verfügung, um den individuellen Anforderungen gerecht zu werden.

Das cidaas Einsteiger-Service-Paket ist kostenfrei.

Jetzt einsteigen

FAZIT

Die Frage, ob man ein Identitätsmanagement einsetzt oder nicht, wird sich zukünftig für die meisten Unternehmen nicht mehr stellen. Egal ob es sich um Kunden, Partner, Mitarbeiter oder gar „Dinge" handelt – alle sind digital vernetzt und erwartet einen reibungslosen und autorisierten Zugriff auf Applikationen, Services und Daten sowie die Wahrung der Datenschutzregulationen.

> Eine Customer Identity Plattform sichert Ihre Identitäten ab

Mit einem Customer Identity und Access Management sichern Sie Ihre Identitäten und Kanäle nicht nur zuverlässig ab und minimieren so die Sicherheitsrisiken, sondern bilden gleichzeitig auch den Grundstock für alle datenschutzrelevanten Themen hinsichtlich der EU-DSGVO.

Warten Sie nicht länger und vereinbaren Sie eine **kostenlose Beratung** - gerne stehen wir Ihnen bei Ihrer digitalen Transformation mit unserer Expertise zur Verfügung.

Im Zeitalter der Digitalisierung hat der Schutz von digitalen Identitäten und Portale immens an Bedeutung gewonnen, denn jede Organisation betreibt mittlerweile eine digitale Präsenz in irgendeiner Form.

Mit cidaas stellen wir Unternehmen eine leistungsstarke Software zur Verfügung, die out-of-the-box alle relevanten Sicherheitsanforderungen hinsichtlich Authentifizierung und Autorisierung bereitstellt sowie die rechtskonforme Aufbewahrung und Bereitstellung personenbezogener Daten gewährleistet.

Sadrick Widmann . Chief Product Officer cidaas

Jetzt Wunschtermin buchen

WIDAS ID GMBH

Maybachstraße 2
71299 Wimsheim
Tel: +49(0)7044 95103-100
Email: contact@widas.de

cidaas

Phone: +49 (7044) 95103 - 100
Mail: sales@cidaas.de
Web: www.cidaas.com