ForgeRock®

Wirtschaft im Wandel – Die 8 wichtigsten Digitalisierungstrends und ihre Auswirkungen

Warum Konsumententrends Consumer Identity and Access Management (CIAM) alternativlos machen

Executive Summary

Acht Digitalisierungstrends prägen derzeit aktiv unsere Wirtschaft und unsere Gesellschaft und verändern dadurch nachhaltig das Umfeld, in dem Unternehmen operieren. Um in Zeiten der Pandemie und darüber hinaus zu überleben und zu florieren, müssen Unternehmen jedem dieser Trends Rechnung tragen.

1. Disruption: Die Erneuerung der Wirtschaft
Die Pandemie hat unsere Welt auf den Kopf gestellt. Für Unternehmen steht damit viel auf dem Spiel: Sie müssen sich heute neu aufstellen, um auch morgen noch Kunden zu gewinnen und zu binden, ihre Verluste zu minimieren und ihr Geschäft zukunftssicher zu machen.

2. Partner-Ökosysteme
Im Rahmen ihrer Neuerfindung schließen sich viele Unternehmen digitalen Ökosystemen mit mehreren Partnern an, um das unstillbare Verlangen der Verbraucher nach einem herausragenden Nutzungserlebnis und hohem Komfort zu erfüllen.

3. „Phygitale" Erlebnisse
Die Verbraucher erwarten ein nahtloses Erlebnis, egal wie und wo sie mit einem Unternehmen interagieren – ob über physische und digitale Kanäle hinweg.

4. Internet der Dinge (IoT)
Der globale IoT-Verbrauchermarkt wird voraussichtlich von 97,50 Milliarden US-Dollar im Jahr 2020 auf schätzungsweise 188,34 Milliarden US-Dollar im Jahr 2026 ansteigen.[1] Das Problem: Viele dieser „Dinge" sind nicht ausreichend geschützt.

5. Cyberkriminalität, Datenschutzverletzungen, Betrug und Übergriffe
Die Zahl der Datenschutzverletzungen, Betrugsfälle, Ransomware-Angriffe sowie Datenübergriffe ist während der letzten Jahre sprunghaft angestiegen und der Höhepunkt scheint noch nicht erreicht.

6. Öffentliche Meinung und Aktivismus
Wir leben in einem Zeitalter des Misstrauens. Die öffentliche Meinung hat sich gewandelt. Verbraucher möchten Kontrolle über ihre persönlichen Daten haben und Unternehmen im Ernstfall zur Verantwortung ziehen können.

7. Datenschutz, Zustimmung und gesetzliche Bestimmungen
Als Antwort auf Forderungen seitens der Bevölkerung haben Regierungen weltweit Gesetze erlassen, um den Umgang mit Daten zu regulieren. Und in kommenden Jahren werden höchstwahrscheinlich weitere folgen.

8. Gen Z, Gen Alpha und das Metaversum
Mit einem Anteil von 32 % an der Weltbevölkerung ist Generation Z heute die zahlenmäßig stärkste Gruppe.[2] Auf sie folgt Generation Alpha, deren Mitglieder zwar noch keine 12 Jahre alt sind, aber bereits Kaufentscheidungen im Wert von über 500 Milliarden Dollar beeinflussen. Gen Z und Gen Alpha werden in den kommenden Jahren nicht mehr nur im Metaversum spielen, sondern auch dort arbeiten, einkaufen und investieren.

Um auf diese acht Trends zu reagieren, nutzen Unternehmen zunehmend Identitätsplattformen der Enterprise-Klasse, die speziell für Customer Identity and Access Management (CIAM), IoT und zukünftige Anwendungsfälle konzipiert sind.

1 https://www.marketdataforecast.com/market-reports/consumer-iot-market
2 https://nypost.com/2020/01/25/generation-z-is-bigger-than-millennials-and-theyre-out-to-change-the-world/

ForgeRock: Der unangefochtene Marktführer für CIAM

ForgeRock Enterprise CIAM – von Gartner, Forrester und KuppingerCole als richtungsweisend und visionär auf dem Gebiet des Consumer Identity and Access Management (CIAM) bezeichnet – ist die einzige Lösung am Markt, die dazu in der Lage ist, alle acht globalen Digitalisierungstrends heute und auch in Zukunft anzugehen.

Mit ForgeRock Enterprise CIAM können Unternehmen:

- ihre Geschäfts- und IT-Strategien überarbeiten, um jegliche Art der Disruption abzufedern und die Anforderungen der Verbraucher mit maximaler Flexibilität und Zuverlässigkeit zu erfüllen.
- in sicheren digitalen Ökosystemen mit mehreren Partnern vernetzt sein.
- ein sicheres und nahtloses Omnichannel-Kundenerlebnis über physische und digitale Kanäle hinweg bieten.
- das Internet der Dinge sichern und die Beziehungen zwischen Benutzern und Dingen regeln.
- sich an die Vorgaben hinsichtlich Datenschutz, Zustimmung und andere gesetzliche Bestimmungen halten und Vertrauen in ihre Marke aufbauen.
- Cyberkriminalität und Betrug erkennen und verhindern.
- ihr Geschäft zukunftssicher machen, damit es auch die Anforderungen der nächsten Generationen erfüllen kann.

Dank ForgeRock können Unternehmen die acht Trends nicht nur angehen, sondern ihnen sogar zuvorkommen. Mit der CIAM-Lösung von ForgeRock eröffnen sich den Unternehmen neue Möglichkeiten der Umsatzsteigerung, da sie die Erwartungen der Verbraucher übertreffen, Risiken und Betrug dank Zero-Trust-Sicherheit minimieren und das Vertrauen in die digitale Welt sowie die Loyalität der Kunden durch die Einhaltung von Datenschutz- und Einwilligungsbestimmungen stärken können.

Inhaltsverzeichnis

Wirtschaft im Wandel – Die 8 wichtigsten Digitalisierungstrends und ihre Auswirkungen

Warum Konsumententrends Consumer Identity and Access Management (CIAM) alternativlos machen

Acht Digitalisierungstrends prägen derzeit aktiv unsere Wirtschaft und unsere Gesellschaft und verändern dadurch nachhaltig das Umfeld, in dem Unternehmen operieren. Um in diesen Zeiten zu überleben und zu florieren, müssen Unternehmen jedem dieser Trends Rechnung tragen.

1

Disruption: Die Erneuerung der Wirtschaft

Um die „Erneuerung der Wirtschaft“ zu verstehen, müssen wir bei der „Disruption der Wirtschaft“ ansetzen. Verbraucher wollen makellose und personalisierte Omnichannel-Erlebnisse. Um dieser Forderung nachzukommen und dem Wettbewerb eine Nasenlänge voraus zu sein, betreiben Wirtschaftsunternehmen einen enormen Aufwand, um neue Dienste zu entwickeln und das Kundenerlebnis zu perfektionieren. Ihr Ziel: die „Disruption“ des Marktes.

70 % der Befragten gaben an, dass disruptives Wachstum ein entscheidender Faktor für den Erfolg ihres Unternehmens sei, aber nur 13 % waren zuversichtlich, dass ihr Unternehmen dieser strategischen Priorität gerecht wird.[3]

Deloitte.

Im Jahr 2005 gelang beispielsweise Amazon eine solche Disruption des Marktes mit seinem Prime-Programm – und dem Versprechen eines kostenlosen Versands innerhalb von zwei Tagen für Mitglieder. Noch heute, mehr als 15 Jahre später, ringen viele andere Händler darum, mit dieser inzwischen üblichen Verbrauchererwartung mitzuhalten.

Zum Wesen der disruptiven Wirtschaft gehört, dass sie sich ständig verändert. Unternehmen finden neue, innovative Wege, um ihre Kunden zu unterstützen und zu begeistern. Die Verbraucher wiederum gewöhnen sich an die Innovationen. Diese werden damit zu Erwartungen, was wiederum die Unternehmen veranlasst, die nächste Neuerung hervorzubringen.

Dieser faszinierende Tanz zwischen Innovation und Erwartung gibt seit über zwei Jahrzehnten den Takt in unserer Gesellschaft an. Vor Pandemiebeginn war die Fähigkeit, makellose, personalisierte Omnichannel-Kundenerlebnisse bereitzustellen, das Maß der Dinge, wenn es um Initiativen zur digitalen Transformation ging. Und das in allen Branchen. Die Planung und Umsetzung dieser Initiativen erstreckte sich in den meisten Unternehmen über mehrere Jahre. Doch mit dem Ausbruch der Pandemie wurden die digitalen Angebote zum Rettungsanker für Menschen und Unternehmen. Quasi über Nacht verkürzte sich der Zeitrahmen für die digitale Transformation von mehreren Jahren auf wenige Wochen. Die Nase vorn hatten dabei die Unternehmen, die bereits über eine modernisierte IT-Infrastruktur und ein digitales Serviceangebot verfügten und in der Lage waren, die Nachfrage der Verbraucher von Tag 1 an zu erfüllen.

3 https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf

Mit der ultimativen Disruption durch die Pandemie wurde die „Erneuerung der Wirtschaft“ geboren.

Weltweit löste die Pandemie einen digitalen Transformationswettlauf aus. Nun, wo Unternehmen mit globalen wirtschaftlichen Unsicherheiten zu kämpfen haben, liefern sie sich ein erbittertes Rennen, um Kunden zu gewinnen und zu binden, ihre Verluste zu minimieren und ihr Geschäft zukunftssicher zu machen.

83 %

der Führungskräfte sind sich einig, dass die Geschäfts- und Technologiestrategien ihres Unternehmens untrennbar miteinander verbunden – ja sogar nicht mehr zu unterscheiden – sind.[4]

accenture

Um wettbewerbsfähig zu bleiben und die Verbraucher in einer digitalisierten Welt zufriedenzustellen, investieren Unternehmen ungeahnte Summen in ihre Neuaufstellung mit dem Ziel, intelligenter, flexibler und widerstandsfähiger zu werden. Sie modernisieren zum Beispiel ihre IT-Infrastrukturen und verlagern möglichst große Teile in die Cloud; sie integrieren IoT-Sensoren, -Beacons und -Geräte; sie implementieren künstliche Intelligenz (KI), maschinelles Lernen (ML) und robotergestützte Prozessautomatisierung (RPA); und sie bauen Digital Twins und Spiegelwelten auf.

An erster Stelle steht dabei stets das Verbrauchererlebnis. Daneben zielen die massiven Anstrengungen hinter der Erneuerung der Wirtschaft aber auch darauf ab, die Unternehmen zukunftsfähig zu machen, damit sie die Welt nicht nur dort abholen, wo uns die Pandemie hingeführt hat, sondern auch unseren weiteren Weg ebnet. Dazu muss die Geschäftsstrategie mit modernen Technologielösungen kombiniert werden.

Der Ausbau der eigenen Zukunftsfähigkeit ist von entscheidender Bedeutung – insbesondere für den Aufbau eines stabilen Unternehmens, das Volatilität und Disruption frühzeitig erkennen und abfedern kann.[5]

Gartner

4 https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Full-Report.pdf
5 Gartner, The C-Suite Guide: Accelerate Digital for Future-Ready Business. Frameworks for composable tech, empowered customers and the future of work, 2021

2

Partner-Ökosysteme

Im Rahmen ihrer Neuaufstellung schließen sich viele Unternehmen digitalen Ökosystemen mit mehreren Partnern an, um das unstillbare Verlangen der Verbraucher nach einem erstklassigen, personalisierten Omnichannel-Erlebnis mit hohem Komfort zu erfüllen.

Laut McKinsey[6] sind sieben der 12 größten Unternehmen der Welt (gemessen an der Marktkapitalisierung) in digitalen Ökosystemen organisiert. Mit Technologien wie Cloud und Anwendungsprogrammierschnittstellen (APIs) verbessern diese Partnernetzwerke die betriebliche Effizienz, Transparenz und Skalierbarkeit, erweitern das Serviceangebot und ermöglichen disruptive Erlebnisse.

Im Gesundheitswesen beispielsweise schließen sich Anbieter, Kostenträger, Händler und andere Branchenvertreter zusammen, um ein digitales Gesundheitsökosystem zu erschaffen, das verschiedene Dienstleistungen in einer praktischen Kundenanwendung vereint. Mit einer einzigen App können Verbraucher zum Beispiel Termine vereinbaren, telemedizinische Sprechstunden wahrnehmen, ihre Testergebnisse einsehen, Rechnungen bezahlen, Anträge einreichen, Vorsorgeerinnerungen und Tipps erhalten und sehen, wann ihre Rezepte abholbereit sind.

Führende Unternehmen haben erkannt, dass die Bündelung ihrer Kräfte und gemeinsame Entwicklung von Lösungen, die ein nahtloses End-to-End-Kundenerlebnis während der gesamten Customer Journey ermöglichen, die Erfolgsstrategie der Zukunft ist. Entscheidend für diese Zusammenarbeit ist, dass diese digitalen Ökosysteme mit mehreren Parteien über angemessene API-Sicherheit verfügen und dass nur ein erforderliches Maß an Zugriff auf Systeme und Daten über Unternehmensgrenzen hinweg gewährt wird.

60 Billionen Dollar

Unsere Untersuchungen zeigen, dass die entstehenden digitalen Ökosysteme bis 2025 für mehr als 60 Billionen US-Dollar Umsatz sorgen könnten – das sind mehr als 30 % des weltweiten Unternehmensumsatzes.[7]

McKinsey & Company

6,7 https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/the-strategy-and-corporate-finance-blog/if-youre-not-building-an-ecosystem-chances-are-your-competitors-are

3

Phygitale Erlebnisse

Die Pandemie hat vieles ausgelöst, unter anderem eine wiederentdeckte Wertschätzung für persönliche Erlebnisse. Gleichzeitig hat sie der Öffentlichkeit die Annehmlichkeiten digitaler Dienste näher gebracht. Heute wollen die Menschen das Beste aus beiden Welten.

In dem Maße, in dem Unternehmen die Möglichkeiten technologiegestützter Produkte und Dienstleistungen neu definieren, werden sie feststellen, dass sie eine aktivere Rolle in der Beziehung zwischen Menschen und Technologie spielen als jemals zuvor.[8]

accenture

Ken Hughes, ein führender Experte für Verbraucher- und Einkaufsverhalten, sagt: „Die menschliche Dimension des Kundenerlebnisses war noch nie so wichtig wie heute. Ein gutes Kundenerlebnis – oder CX (Customer Experience) – ist nicht nur eine Frage des Komforts, sondern vor allem der Beziehung. Die Digitalisierung mag uns Effizienz bringen, aber echte Verbundenheit entsteht erst durch die einfühlsame, menschliche Note. Bytes und Beziehung – beide sind gleichermaßen wichtig.“[9]

Omnichannel schließt heute alle Kanäle ein, auch den physischen Kanal. Die Verbraucher wünschen sich ein nahtloses, personalisiertes Erlebnis, das genau dort anknüpft, wo sie zuletzt aufgehört haben – egal, wie sie mit einem Unternehmen interagieren. Um diesem Wunsch zu entsprechen, kreieren Unternehmen „phygitale“ Erlebnisse – maßgeschneiderte Customer Journeys mit einer Kombination aus physischen und digitalen Elementen.

Physisch + Digital ist das neue Maß der Dinge. Wir gehen davon aus, dass führende Unternehmen in den nächsten 18 bis 24 Monaten den milliardenschweren Trend aufgreifen und Wege finden werden, um mithilfe von am Menschen orientiertem Design und digitaler Technologie personalisierte, digital angereicherte Interaktionen in großem Maßstab zu gestalten.[10]

Deloitte.

Einige Gesundheitsdienstleister nutzen zum Beispiel Apps und Geolokalisierung, um Patienten in Echtzeit den Weg durch große medizinische Einrichtungen zu ihrem Termin zu weisen. Ein anderes Beispiel sind Einzelhändler, die Kunden während ihres Aufenthalts im Geschäft SMS schicken, um ihnen personalisierte Angebote zu unterbreiten oder sie zum Standort von Produkten zu führen, die diese zuvor online gesucht haben. Auch Restaurants bieten phygitale Erlebnisse, zum Beispiel indem sie QR-Codes zum Aufrufen von Speisekarten einsetzen. Außerdem nutzen sie Apps, mit denen die Kunden ihre Rechnung ganz einfach aufteilen und bezahlen können. Phygitale Erlebnisse haben auch in Bekleidungsgeschäften Einzug gehalten. Einige Einzelhandelsunternehmen wie Macy's haben in ihren Filialen intelligente Augmented-Reality-Spiegel (AR) installiert, mit denen die Kunden sehen können, wie ihnen die Kleidungsstücke stehen, bevor sie diese anprobieren.

Schon in wenigen Jahren wird die Integration von digitalen und physischen Erlebnissen aus unserem Alltag nicht mehr wegzudenken sein. Voraussetzung für solch phygitale Erlebnisse ist es, den Kunden an jedem Touchpoint zu erkennen und Sicherheit sowie Vertrauen zu schaffen.

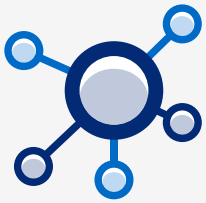
8 https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Full-Report.pdf
9 https://kenhughes.info/wp-content/uploads/2020/11/The-captive-economy-2021.pdf
10 https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf

4

Intelligente Geräte und das Internet der Dinge (IoT)

Intelligente Geräte und das Internet der Dinge (Internet of Things, IoT) sind mittlerweile allgegenwärtig, da Unternehmen aller Branchen neue Angebote und phygitale Erlebnisse entwickeln. Laut Market Data Forecast[11] wird der globale IoT-Verbrauchermarkt von 97,50 Milliarden Dollar im Jahr2020 auf voraussichtlich 188,34 Milliarden Dollar im Jahr 2026 anwachsen.

Von phygitalen intelligenten Spiegeln bis hin zu Thermometern, Matratzen, Autos, Schuhen und Spielwaren – Dreh- und Angelpunkt des Verbrauchergeschäfts sind zunehmend IoT-Dinge, die von ihnen erfassten Daten und die damit verbundenen Apps.



IoT-Geräte zählen zu den unsichersten vernetzten Maschinen, sind aber gleichzeitig in unserem Leben allgegenwärtig.[12]

WORLD ECONOMIC FORUM

Philips hat zum Beispiel eine Produktlinie von intelligenten Glühbirnen namens Philips Hue entwickelt. Die Glühbirnen lassen sich mit der mobilen Philips Hue App verbinden, mit der Nutzer Lichteinstellungen wie Helligkeit, Farbe oder Stimmung vornehmen können. Sie können die Glühbirnen außerdem mit Geräten wie dem Amazon Echo oder dem Google Nest verbinden, um die Beleuchtung freihändig oder von unterwegs aus zu steuern.

Obgleich das IoT das Leben der Verbraucher verbessert und Unternehmen dabei hilft, sich mit neuartigen Dienstleistungsangeboten von der Konkurrenz abzuheben, ist es leider traurige Realität, dass die meisten Dinge im IoT nicht sicher sind und in missbräuchlicher Weise verwendet werden können. Im ersten Halbjahr 2021 haben sich die IoT-Cyberangriffe im Vergleich zum Vorjahr mehr als verdoppelt und führten zu rund 1,51 Milliarden Datenschutzverletzungen, ein deutlicher Anstieg gegenüber den 639 Millionen im Jahr 2020.[13]

Und da die Folgen von IoT-Hacking und Datenschutzverletzungen verheerend sein können, muss der Sicherheit von IoT-Identitäten und deren Daten oberste Priorität eingeräumt werden.

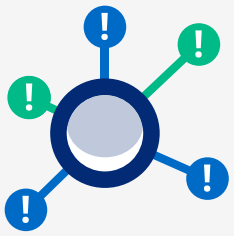
11 https://www.marketdataforecast.com/market-reports/consumer-iot-market
12 https://www.weforum.org/agenda/2021/08/threats-to-iot-devices-are-constantly-evolving-but-is-security-keeping-up/
13 https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky

5

Cyberkriminalität, Datenschutzverletzungen, Betrug und Übergriffe

In dem Maße, in dem die digitale Entwicklung an Fahrt aufnimmt, gewinnen auch die neuen Taktiken der Cyberkriminalität und Cyberkriegsführung an Dynamik. Es gibt heutzutage nichts Schlimmeres für ein Unternehmen als Hackerangriffe, Datenschutzverletzungen oder Ansehensverluste aufgrund unzureichender Sicherheits- und Datenmanagementpraktiken. Gerade in den letzten Jahren hat die Zahl der Datenschutzverletzungen, Betrugsfälle, Ransomware- und Phishing-Angriffe sowie Übergriffe einen neuen Höchststand erreicht.

Angesichts der zu erwartenden Zunahme von intelligenten Geräten, 5G, Edge Computing und künstlicher Intelligenz wird es noch mehr Daten und vernetzte Knoten geben, die die Angriffsfläche weiter vergrößern.[14]



Deloitte.

85% Bei fast 85 % der erfolgreichen Datenschutzverletzungen handelte es sich um Betrug an Menschen.[15]

80% Hauptangriffspunkt sind Webanwendungen, verantwortlich für mehr als 80 % der Datenschutzverletzungen.[16]

61% aller Datenschutzverletzungen sind das Ergebnis von Methoden wie Phishing, bei denen Anmeldedaten gestohlen werden.[17]

2 Mrd. 2 Mrd. Datensätze mit Benutzernamen und Passwörtern wurden 2021 kompromittiert. [18]

136% IoT-Cyberangriffe sind allein in der ersten Hälfte des Jahres 2021 um 136 % gestiegen.[19]

14 https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf
15 https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/
16 https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf
17 https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/
18 https://www.forgerock.com/resources/analyst-report/2022-forgerock-consumer-identity-breach-report
19 https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/

Die häufigsten Türen, die den Zugang zu einem IT-System öffnen, sind Benutzernamen, Passwörter und personenbezogene Daten. Sie gehören zu den begehrtesten Informationen unter Cyberkriminellen.

Dies sind einige erwähnenswerte Beispiele aus jüngster Zeit. Im Jahr 2019 gelang es Hackern, mit einem gestohlenen Passwort bei SolarWinds einzudringen. Davon betroffen waren bis zu 18.000 Kunden des Unternehmens, darunter Fortune-500-Unternehmen und US-Regierungsstellen. Im Jahr 2020 zahlte die US-Regierung angeblich 400 Milliarden Dollar an betrügerisch bezogener Arbeitslosenunterstützung an einen internationalen Verbrecherring.[20] Im Jahr 2021 zahlte der deutsche Chemielieferant Brenntag ein Lösegeld in Höhe von 4,4 Millionen Dollar, um 150 GB an gestohlenen medizinischen Informationen und anderen vertraulichen Daten wiederzuerlangen.[21] Im selben Jahr waren 47 Unternehmen aus verschiedenen Branchen von einer Datenschutzverletzung bei Microsoft Power Apps betroffen, bei der 38 Millionen Datensätze mit personenbezogenen Daten (PII) offengelegt wurden.[22]

Zwar wurden in den letzten Jahren Fortschritte gemacht, aber die rechtlichen Konsequenzen für Datenschutzverletzungen und Übergriffe blieben oft hinter den Erwartungen der Verbraucher zurück. Hinzu kommt, dass Verbraucher im Falle eines Diebstahls personenbezogener Daten mit den Entschädigungs- und Wiedergutmachungsleistungen, die ihnen von Unternehmen angeboten werden, äußerst unzufrieden sind.

Die Menschen sind desillusioniert. Mehr als ein Jahrzehnt, in dem immer wieder über Datenschutzverletzungen berichtet wurde, hat nicht nur die Art und Weise beeinflusst, wie die Menschen Unternehmen wahrnehmen und mit ihnen interagieren, sondern auch, was sie in Bezug auf Sicherheit, Zugriff, Kontrolle und Verwendung ihrer personenbezogenen Daten erwarten.

Werden Unternehmen ihrer Verantwortung gegenüber ihren Kunden nicht gerecht, sind nicht nur enttäuschte Kunden die Folge. Das Fehlverhalten schafft zudem eine Gesellschaft, die von dem integrierten Innovationsmodell, auf das sich Unternehmen für ihr Wachstum verlassen, desillusioniert ist.[23]

accenture

20 https://www.forbes.com/sites/jackkelly/2021/06/12/the-most-brazen-400-billion-unemployment-funds-heist-in-history/?sh=279ec76a2020
21 https://heimdalsecurity.com/blog/chemical-distributor-brenntag-says-what-data-was-stolen-during-the-ransomware-attack/
22 https://healthitsecurity.com/news/microsoft-data-breach-exposes-38m-records-containing-pii
23 https://www.accenture.com/t20180227T215953Z__w__/us-en/_acnmedia/Accenture/next-gen-7/tech-vision-2018/pdf/Accenture-TechVision-2018-Tech-Trends-Report.pdf#zoom=50

6

Öffentliche Meinung und Aktivismus

Unsere Gesellschaft erlebt ein Zeitalter des Misstrauens. So sind sich die Menschen der weitreichenden Möglichkeiten in Bezug auf das Sammeln von Daten über Suchmaschinen, Cookies und „IoT-Dinge“ sowie der potenziellen Gefahren durch Cyberangriffe wie Phishing und Betrug stärker bewusst. Das Pew Research Center fasst dies folgendermaßen zusammen: „Sie sind besorgt, verwirrt und haben das Gefühl, keine Kontrolle über ihre persönlichen Daten zu haben.“[24]

Laut unserer Umfrage sind die wichtigsten Faktoren für die Weitergabe persönlicher Daten an ein Unternehmen die sichere Erfassung und Speicherung (63 %), gefolgt von der Kontrolle über die übermittelten Daten (57 %) und dem Vertrauen in das Unternehmen (51 %). Wenn ein Unternehmen ihnen dies nicht zusichern kann, werden sie sich anderweitig umsehen..[25]

Mehrere Studien von Organisationen wie dem Pew Research Center, der Agentur der Europäischen Union für Grundrechte, EY, PwC, Salesforce und RSA haben ergeben:

54% der Verbraucher sagen, dass sie durch COVID-19 bewusster mit ihren persönlichen Daten umgehen als vor der Pandemie.[26]

54% der Kunden sagen, dass es für die Unternehmen schwieriger denn je ist, ihr Vertrauen zu gewinnen.[27]

81% der Verbraucher sagen, dass die potenziellen Risiken, die sich aus der Datenerfassung durch Unternehmen ergeben, die Vorteile überwiegen.[28]

24 https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/
25, 26 https://assets.ey.com/content/dam/ey-sites/ey-com/es_es/topics/resilient-enterprise/ey-global-consumer-privacy-study-2020-single-pages.pdf
27 https://www.salesforce.com/form/pdf/state-of-the-connected-customer-3rd-edition/
28 https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/
29 https://fra.europa.eu/en/news/2020/how-concerned-are-europeans-about-their-personal-data-online

6 Öffentliche Meinung und Aktivismus

41% der Einwohner in der Europäischen Union wollen keine persönlichen Daten an Privatunternehmen weitergeben.[29]

64% der Amerikaner geben nicht dem Hacker, sondern dem Unternehmen die Schuld, wenn ihre Daten gehackt werden.[30]

83% der Australier wünschen sich, dass die Regierung ihre Daten besser schützt.[31]

Wie die obigen Statistiken zeigen, ist die öffentliche Meinung in die Defensive gegangen, wodurch das Zusammenspiel zwischen Wirtschaft und Gesellschaft an Bedeutung gewinnt. Die Gesellschaft treibt Forderungen nach geschäftlicher Transparenz und gesetzlichen Bestimmungen mittlerweile maßgeblich voran.

Max Schrems, ein Aktivist und Anwalt, reichte beispielsweise Klagen gegen Facebook – jetzt Meta Inc. – wegen Verstößen gegen den Datenschutz und wegen der Unzulänglichkeiten der Europäischen Union (EU) und des US-amerikanischen Privacy Shields ein. Der Gerichtshof der Europäischen Union (EuGH) entschied in zwei Fällen zugunsten von Schrems und hat damit den Umgang von Unternehmen mit Nutzerdaten weltweit verändert.

> **Vertrauen und Akzeptanz gehen bei der nächsten Generation von Produkten und Dienstleistungen Hand in Hand.**[32]
>
> accenture

Ein weiteres Beispiel ist die Aussage der Facebook-Whistleblowerin Frances Haugen, die enthüllte, dass das Unternehmen es versäumt hat, auf Forschungsergebnisse zu reagieren, die zeigen, dass die bei Instagram und Facebook verwendeten Algorithmen und Taktiken für junge Mädchen und Teenager schädlich sind – neben anderen bedeutsamen Enthüllungen. Diese Aussage hat in den USA eine überparteiliche Forderung nach regulatorischen Maßnahmen ausgelöst. Sie untermauert auch den von der EU vorgeschlagenen Digital Services Act (DSA), das Gesetz über digitale Dienste, das darauf abzielt, illegale Inhalte, einschließlich Falschinformationen, strikt einzuschränken und die High-Tech-Industrie zu zwingen, die Algorithmen, die personenbezogene Daten sammeln und die Inhalte für die Nutzer bestimmen, transparenter zu machen.[33]

30 https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf
31 https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey#:~:text=Eighty%2Dthree%2-0percent%20of%20Australians,feel%20it%20is%20poorly%20protected.
32 https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Full-Report.pdf
33 https://fortune.com/2021/11/08/facebook-whistleblower-european-parliament-big-tech-eu/

7

Datenschutz, Zustimmung und gesetzliche Bestimmungen

Verbraucher sind heutzutage besser über die Sammlung und Nutzung, aber auch den Missbrauch ihrer persönlichen Daten informiert und fordern deshalb mehr Sicherheit, Transparenz, Datenschutz und Kontrolle. Als Reaktion darauf haben Regierungen auf der ganzen Welt eine Vielzahl von Datenschutzbestimmungen ausgearbeitet und verabschiedet. Zum Beispiel:

Australien Consumer Data Right (CDR) und Privacy Act Amendment (Notifiable Data Breaches)

Bahrain: Gesetz zum Schutz personenbezogener Daten

Brasilien: Lei Geral de Proteçao de Dados (LGPD)

Kanada: Digital Charter Implementation Act (Verabschiedung ausstehend)

Chile: Datenschutzgesetzt (Ley 19,628)

China: Gesetz zum Schutz personenbezogener Daten (Personal Data Protection Law, PDPL), (Verabschiedung ausstehend)

Europäische Union: Datenschutz-Grundverordnung (DSGVO)

Indien: Gesetz zum Schutz personenbezogener Daten (Personal Data Protection Bill, PDPB), (Verabschiedung ausstehend)

Israel: Datensicherheitsbestimmungen

Japan: Gesetz zum Schutz personenbezogener Daten

Kenia: Datenschutzgesetz

Qatar: Gesetz Nr. 13

Südafrika: Gesetz zum Schutz personenbezogener Daten (Protection of Personal Information Act, POPIA)

Südkorea: Gesetz zum Schutz personenbezogener Daten

Schweiz: Datenschutzgesetz

Thailand: Gesetz zum Schutz personenbezogener Daten (Personal Data Protection Act, PDPA)

USA: California Consumer Privacy Act (CCPA) und California Privacy Rights Act (CPRA)

USA: Colorado Privacy Act (CPA)

USA: New York SHIELD Act

USA: Virginia Consumer Data Protection Act (CDPA)

Türkei: Gesetz zum Schutz personenbezogener Daten (Nr. 6698)

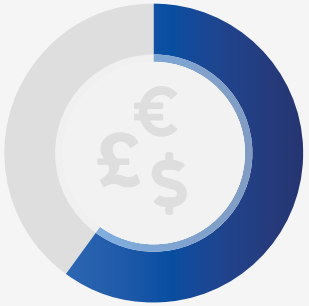
Wenngleich es leichte Abweichungen gibt, verlangen die meisten dieser Bestimmungen, dass Unternehmen Daten sicher aufbewahren und die Betroffenen benachrichtigen, wenn es zu einer Datenschutzverletzung gekommen ist. Die 2016 verabschiedete DSGVO ist die umfassendste und weitreichendste Verordnung. Viele andere Regierungen haben ihre Gesetze nach diesem Vorbild gestaltet. Die DSGVO-Richtlinien besagen unter anderem, dass:

- Verbraucher einer Nutzung ihrer persönlichen Daten eindeutig zustimmen müssen und diese Zustimmung auch ebenso leicht wieder zurücknehmen können.
- alle persönlichen Daten dem Verbraucher zur Verfügung gestellt und auf Anfrage gelöscht werden müssen.
- Datenschutzverletzungen innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls gemeldet werden müssen.
- das Sammeln und die Nutzung von Daten seitens eines Unternehmens unter strengen Sicherheitsauflagen erfolgen muss.

113.5 %

Zwischen Juli 2020 und Juli 2021 ist die Zahl der Verstöße gegen die DSGVO um 113,5 % gestiegen.[34]

Wie wichtig die Einhaltung der Datenschutzbestimmungen ist, wissen auch die Verantwortlichen in den Unternehmen. Zwischen Juli 2020 und Juli 2021 ist die Zahl der Verstöße gegen die DSGVO um 113,5 % gestiegen.[35] So wurde Amazon im Jahr 2021 mit einer Geldstrafe in Höhe von 746 Millionen Euro (888 Millionen Dollar) für Verstöße gegen die DSGVO belegt – das höchste jemals verhängte Bußgeld.



Um Bußgelder zu vermeiden und das Vertrauen der Nutzer zu fördern, gehen 60 % der Unternehmen von einem Anstieg ihrer Datenschutzausgaben im Jahr 2022 aus.[36]

Es steht zu erwarten, dass sich die Vorschriften zum Schutz von Daten und Privatsphäre im Zuge der Verhandlungen zwischen Wirtschaft und Gesellschaft in den kommenden Jahren immer weiter entwickeln werden. Mehrere Länder diskutieren zudem über Ransomware-Gesetze und einen globalen Datenschutzstandard.

Zum Erhalt und Aufbau des verbraucherseitigen Vertrauens müssen Unternehmen diese Vorschriften einhalten und den Verbrauchern die Kontrolle über ihre Daten zurückgeben.

34, 35 https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/
36 https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf

8

Gen Z, Gen Alpha und das Metaversum

Millennials sind seit geraumer Zeit in aller Munde. Führende Unternehmen haben jedoch bereits ein Auge auf die Zukunftsmacher der Generation Z (geboren zwischen 1997 und 2010) und der Generation Alpha (geboren zwischen 2010 und 2028) geworfen.

> **Die Generation Z wird bald die größte Verbrauchergruppe sein – und Marken, die ein Stück von diesem Kuchen abhaben wollen, müssen ihre Vorlieben und Erwartungen an digitale Erlebnisse verstehen.[34]**
>
> INSIDER INTELLIGENCE

Mit einem Anteil von 32 % an der Weltbevölkerung ist Generation Z heute die zahlenmäßig stärkste Gruppe, noch vor den Millennials und den Baby Boomers.[38] Diese Generation übt einen starken Einfluss auf Kaufentscheidungen aus mit einer jährlichen Kaufkraft von 143 Milliarden US-Dollar.[39]

Gen Z – aufgewachsen im Zeitalter von Computern, Mobiltelefonen, Tablets und einer Vielzahl von Social Media-Plattformen – sind echte Digital Natives. Untersuchungen von WP Engine zufolge halten es 52 % der Gen Z nicht länger als vier Stunden ohne Internetzugang aus, bevor sie sich unwohl fühlen.[40] Diese technologieaffine Generation macht zudem keinen Unterschied mehr zwischen physischen und digitalen Kanälen. Und während sich die Millennials noch über rund um die Uhr verfügbare, unmittelbare, nahtlose, vorhersehbare und persönliche Erlebnisse freuten, setzt die Generation Z diese schlichtweg voraus. Sie ist außerdem sensibler im Umgang mit ihren persönlichen Daten, da sie in einer Zeit immenser Datenschutzverletzungen aufwächst.

143 Milliarden US-Dollar

Die Generation Z hat gegenwärtig eine Kaufkraft von 143 Milliarden US-Dollar pro Jahr und großen Einfluss auf die Kaufentscheidungen der Haushalte.[41]

Der Gen Z dicht auf den Fersen ist die Gen Alpha, die Kinder der Millennials. Die ältesten Mitglieder der Gen Alpha sind noch keine 12 Jahre alt, dennoch beeinflussen sie bereits Kaufentscheidungen im Wert von über 500 Milliarden US-Dollar. Diese Generation ist auf sofortige Belohnung programmiert.[42]

38 https://nypost.com/2020/01/25/generation-z-is-bigger-than-millennials-and-theyre-out-to-change-the-world/
39 https://www.lexingtonlaw.com/blog/credit-cards/generation-z-spending-habits.html
40 https://wpengine.com.au/gen-z-aus/
41 https://www.lexingtonlaw.com/blog/credit-cards/generation-z-spending-habits.html
42 https://www.spectrapartnership.com/shakeout-6-trends-shaping-generation-alpha-part-1/

8 Gen Z, Gen Alpha und das Metaversum

Ihr Spielzeug besteht aus vernetzten IoT-Dingen. Sie interagiert mit der Welt durch Augmented Reality (AR) und Virtual Reality (VR). Und wenn Gen Alpha Fragen hat, weiß Alexa von Amazon die Antwort.

Beide, Generation z und Generation Alpha, legen größeren Wert auf das Erlebnis als auf die Marke. Aufgrund dieser Tatsache sowie ihres Einflusses und ihrer digitalen Kompetenz haben führende Unternehmen ihr Ohr am Puls der Gen Z und Gen Alpha und entwickeln dementsprechend ihre Produkt-Roadmaps. Dazu gehört auch die Innovation von Verbraucherdienstleistungen und Dingen innerhalb von Metaversen.

Das Konzept des Metaversums gibt es zwar schon seit einiger Zeit, aber die Entwicklung steckt noch in den Kinderschuhen.
Das Metaversum ist mit einem Videospiel vergleichbar. Es beherbergt Plattformen von Drittanbietern, in die Benutzer nahtlos ein- und austreten können und mit denen sie über eine ganze Reihe verbundener Geräte wie etwa VR-Headsets interagieren können. Innerhalb des nächsten Jahrzehnts werden Gen Z und Gen Alpha nicht mehr nur in Metaversen spielen, sondern auch in Metaversen lernen, arbeiten und einkaufen sowie in Dinge und Immobilien aus Metaversen als Teil ihrer Altersvorsorge investieren.[43]

Trotz ihres noch jungen Alters haben Gen Z und Gen Alpha einen spürbaren Einfluss auf die Wirtschaft, die Gesellschaft und die Zukunft. Die Welt, die sie für sich beeinflussen und beanspruchen, macht alle acht Trends umso bedeutender.

43 https://www.wsj.com/articles/investors-see-promising-new-world-in-metaverse-11638455401

Das Gebot der nächsten Jahre

Die zuvor beschriebenen acht Trends sind ohne Frage eine treibende Kraft. Um ihnen zu begegnen, müssen Unternehmen:

- ihre Geschäfts- und IT-Strategien überarbeiten, um jegliche Art der Disruption abzufedern und die Anforderungen der Verbraucher mit maximaler Flexibilität und Zuverlässigkeit zu erfüllen.
- in sicheren digitalen Ökosystemen mit mehreren Partnern vernetzt sein.
- ein sicheres und nahtloses Omnichannel-Kundenerlebnis über physische und digitale Kanäle hinweg bieten.
- das Internet der Dinge sichern und die Beziehungen zwischen Benutzern und Dingen regeln.
- sich an die Vorgaben hinsichtlich Datenschutz, Zustimmung und andere gesetzliche Bestimmungen halten und Vertrauen in ihre Marke aufbauen.
- Cyberkriminalität und Betrug erkennen und verhindern.
- ihr Geschäft zukunftssicher machen, damit es auch die Anforderungen der nächsten Generationen erfüllen kann.

Führende Unternehmen setzen deshalb auf eine CIAM-Plattform der Enterprise-Klasse.

CIAM trägt maßgeblich dazu bei, dass die digitalen Unternehmen von heute Kunden gewinnen und an sich binden können. Die Kunden wiederum erhalten die nötigen Sicherheits- und Personalisierungsfunktionen, um mit dem Unternehmen zu interagieren und Geschäfte zu machen.[44]

FORRESTER®

44 https://www.forrester.com/report/now-tech-customer-identity-and-access-management-ciam-q2-2020/RES160459?objectid=RES160459

Wie Sie die acht Trends mit Enterprise CIAM meistern können

Consumer Identity and Access Management (CIAM) ist unverzichtbar, um diesen acht Trends zu begegnen. Einfach gesagt: CIAM versetzt Unternehmen in die Lage, Verbraucher- und IoT-Identitäten und -Daten zu erfassen, zu verwalten und zu schützen, Verbrauchern und IoT einen angemessenen Zugriff auf Anwendungen und Dienste zu ermöglichen und Verbrauchern die Kontrolle über ihre Datenschutz- und Datenfreigabeeinstellungen zu geben. Enterprise CIAM wurde eigens dafür entwickelt, Milliarden von Identitäten zu unterstützen und die oben genannten Funktionen im Internetmaßstab bereitzustellen.

Die folgende Tabelle zeigt die einzelnen Trends und wie Enterprise CIAM diesen begegnet.

TREND UND ANFORDERUNG	CIAM-FUNKTION
1. Die Erneuerung der Wirtschaft Erfordert eine Modernisierung der IT, um jegliche Disruption abzufedern und die Forderungen der Verbraucher mit maximaler Flexibilität und Zuverlässigkeit zu erfüllen	Eine Enterprise CIAM-Plattform beinhaltet die neuesten Technologien mit Funktionen, die sich im Handumdrehen aktualisieren und ändern lassen, um die Erneuerung zu erleichtern. Enterprise CIAM lässt sich außerdem mühelos in Legacy- und Cloud-Umgebungen über die gesamte hybride IT hinweg integrieren und dient als Single Point of Truth für das Identitätsmanagement. Zudem lässt sich die Lösung ganz einfach skalieren, um Millionen oder sogar Milliarden von Identitäten zu unterstützen, ohne dass kostspielige Add-Ons von Drittanbietern erforderlich sind oder es zu Störungen kommt. Und das Wichtigste: CIAM der Enterprise-Klasse ist einfach zu aktualisieren.
2. Partner-Ökosysteme Erfordert neben sicheren Integrationen und der gemeinsamen Nutzung von Daten ein hohes Vertrauen zwischen den Partnerorganisationen	Enterprise CIAM versetzt Unternehmen in die Lage, ihr Geschäft gemeinsam mit Partnern auszubauen und zu erweitern. Sie können dabei auf vorgefertigte Integrationen (über REST-API-Funktionen) zurückzugreifen, die sich überall einbinden lassen. Diese sind nötig, um erstklassige Erlebnisse zu kreieren Enterprise CIAM schützt zudem die APIs und Zugangspunkte, umfasst vorintegrierte Lösungen von Technologiepartnern und gewährleistet Datenschutz und Sicherheit.

TREND UND ANFORDERUNG	CIAM-FUNKTION
3. Phygitale Erlebnisse Erfordert die Bereitstellung nahtloser Erlebnisse über physische und digitale Kanäle hinweg	Mit einer Enterprise CIAM-Plattform können Unternehmen auf einfache Weise personalisierte Omnichannel-Erlebnisse bereitstellen. Die Identität jedes Nutzers bleibt dabei über mehrere Geräte hinweg die gleiche. Möglich ist dies, da Enterprise CIAM eine Vielzahl von technischen Anforderungen erfüllt, die sich von Gerät zu Gerät unterscheiden, z. B. zwischen Smartwatch, Tablet oder Laptop. Enterprise CIAM kann zudem Daten aus mehreren Systemen zusammenführen und so eine einheitliche Sicht auf den Verbraucher liefern. Ausgehend dieser Gesamtübersicht können dann individuelle Kundenerlebnisse in physischen und digitalen Umgebungen entwickelt werden. Enterprise CIAM vereinfacht außerdem die Registrierung und Anmeldung sowie die Verwaltung von Passwörtern und Einstellungen für ein optimales Nutzungserlebnis.
4. Intelligente Geräte und das Internet der Dinge (IoT) Erfordert IoT-Identitätssicherheit, IoT-Datensicherheit und die Fähigkeit, die Beziehungen zwischen Menschen und ihren Dingen zu verwalten	Mit einer Enterprise CIAM-Plattform können Unternehmen das Internet der Dinge in ihr Produktangebot integrieren – und das mit dem angemessenen Maß an Sicherheit. So ist beispielsweise für eine vernetzte Glühbirne ein anderes Maß an Sicherheit erforderlich als für ein Fahrzeug oder einen Atomreaktor. Enterprise CIAM hilft außerdem dabei, IoT-Daten zu schützen und sie mit der Identität einer Person zu verknüpfen. Unternehmen können eine CIAM-Plattform ferner nutzen, um die Beziehungen zwischen IoT-Dingen und den Menschen, die diese Dinge besitzen oder nutzen, zu verwalten.
5. Cyberkriminalität, Datenschutzverletzungen, Betrug und Übergriffe Erfordert, dass Unternehmen Cyberkriminalität und Betrug erkennen und sich davor schützen	Enterprise CIAM-Plattformen unterstützen moderne Sicherheitsfunktionen und -modelle, die auf der Annahme beruhen, dass keine Person bzw. kein Ding vertrauenswürdig ist und daher laufend überprüft werden muss. Mit Enterprise CIAM können Sicherheitsmaßnahmen basierend auf dem Zero-Trust-Modell oder der CARTA-Strategie (Continuous Adaptive Risk and Trust Assessment) umgesetzt werden, bei denen die Identität als Sicherheitsgrenze dient, um das Zugriffsrisiko kontinuierlich zu analysieren. Darüber hinaus können Unternehmen die Notwendigkeit einer Passworteingabe während des Anmeldevorgangs aufheben. Allein dadurch lassen sich Phishing-Angriffe, Credential Stuffing und Man-in-the-Middle-Angriffe auf Sitzungen verhindern. Enterprise CIAM beinhaltet außerdem eine Cloud-Architektur, in der die Daten der einzelnen Unternehmen voneinander isoliert sind, um höchste Sicherheit zu gewährleisten.

TREND UND ANFORDERUNG	CIAM-FUNKTION
6. Öffentliche Meinung und Aktivismus Erfordert, Vertrauen aufzubauen und den Verbrauchern die Kontrolle zu geben	Mit Enterprise CIAM können Unternehmen Vertrauen und Loyalität aufbauen, indem sie ihren Kunden die Kontrolle über ihre Daten und Einstellungen ermöglichen und deren Wunsch nach Datenlöschung erfüllen. Darüber hinaus trägt Enterprise CIAM, wie weiter unten erläutert, mit seinen umfangreichen Cybersecurity-Funktionen dazu bei, das Ansehen von Unternehmen zu bewahren.
7. Datenschutz, Zustimmung und gesetzliche Bestimmungen Erfordert die Einhaltung von Datenschutz-, Zustimmungs- und anderen gesetzlichen Bestimmungen	Enterprise CIAM-Plattformen erleichtern Unternehmen die Einhaltung gesetzlicher Vorschriften mit Funktionen, die den Verbrauchern die Kontrolle über Daten, Datenschutz und Zustimmung geben. Ebenso helfen sie, die Anforderungen an Datenhoheit und Datenresidenz zu erfüllen.
8. Gen Z, Gen Alpha und das Metaversum Erfordert die Berücksichtigung aller oben genannten Trends sowie die Fähigkeit, neue Trends aufzugreifen	Enterprise CIAM versetzt Unternehmen in die Lage, Kundenerlebnisse zu personalisieren und Customer Journeys entsprechend den persönlichen und generationsspezifischen Vorlieben zu gestalten. Zudem kann Enterprise CIAM mit dem Verbraucher mitwachsen, d. h. beginnend als Kind oder Mitglied des elterlichen Kontos und gefolgt von einem eigenen Konto in späteren Jahren. Ferner lässt sich Enterprise CIAM mühelos mit anderen Technologien – neuen wie alten – integrieren.

Warum ältere und selbstentwickelte Identitätssysteme unzureichend sind

Aus Kostengründen haben viele Unternehmen versucht, ihre bestehenden IAM-Systeme für die Mitarbeiter so zu modifizieren, dass sie den Trends und Anforderungen Rechnung tragen, anstatt in eine unternehmensweite CIAM-Plattform zu investieren. Die Ergebnisse sind jedoch alles andere als ideal, wie die Disruption im Zuge der Pandemie gezeigt hat.

BMW konsolidierte zum Beispiel 20 verschiedene IAM-Systeme auf einer ForgeRock-Plattform. Dadurch konnten erhebliche Kosteneinsparungen sowie eine schnellere Markteinführung, eine bessere Skalierbarkeit und eine höhere Compliance erzielt werden.

Herkömmliche IAM-Systeme wurden für bestimmte Anwendungsfälle der Mitarbeiter entwickelt. Sie sind nicht darauf ausgelegt, Millionen oder gar Milliarden von Kunden-, Partner- und IoT-Identitäten zu sichern und zu verwalten – ganz zu schweigen von deren Datenflut. Des Weiteren wurde bei den bestehenden IAM-Systemen weder Wert auf nahtlose Omnichannel-Erlebnisse gelegt, noch unterstützen sie die gesetzlichen Bestimmungen, wie DSGVO, CCPA und CDR, oder mindern die Gefahr moderner Cyberkriminalität und Betrugsmethoden. Auch erfüllen die bestehenden IAM-Lösungen keine modernen Standards, wodurch sich ein Partner-Ökosystem nur schwer einbinden lässt. Noch dazu ist es äußerst schwierig und kostspielig, sie aufzurüsten – und dennoch ist ein Upgrade unumgänglich, damit sie die grundlegendsten Anwendungsfälle unserer Zeit abdecken, ganz zu schweigen von den acht Trends.

Statt ihr traditionelles IAM-System zu modifizieren, um so den acht Trends gerecht zu werden und sich für die Zukunft vorzubereiten, sollten Unternehmen lieber eine umfassende und speziell zu diesem Zweck entwickelte Enterprise CIAM-Plattform einsetzen.

„Mit ForgeRock können wir nicht nur die Customer Journeys unserer Kunden heute optimieren, sondern auch flexibel auf Veränderungen reagieren, wenn die Branche in den kommenden Jahren verstärkt zu einem Ökosystemmodell wechselt."

Chris Worle, Chief Digital Officer

HARGREAVES LANSDOWN

Der Business Case für Enterprise CIAM

Eine Enterprise CIAM-Plattform ist die Basis für Erneuerung, Sicherheit und Disruption. Führende Unternehmen setzen darauf, um allen acht Trends zu begegnen und gleichzeitig ihre IT-Ressourcen zu entlasten. Mit einer Enterprise CIAM-Lösung können sie die Kundenakquise beschleunigen, das Kundenerlebnis verbessern und ihre Kunden schützen.

Unternehmen, die eine CIAM-Lösung (Customer Identity and Access Management) mit integrierter Betrugserkennung und passwortloser Authentifizierung einführen, werden die Kundenabwanderung bis 2025 um mehr als die Hälfte reduzieren können.[45]

Gartner®

45 https://www.gartner.com/en/documents/4009255-innovation-insight-for-customer-identity-and-access-management

1. Schnellere Kundenakquise

Moderne CIAM-Plattformen erleichtern die Erneuerung, indem sie Legacy- und Cloud-Umgebungen innerhalb der hybriden IT integrieren und so als Single Source of Truth für Identitäten im gesamten Unternehmen dienen. Darüber hinaus beseitigen Enterprise CIAM-Funktionen die Hürden zwischen Unternehmen und ihren Kunden mit Funktionen wie einem einfachen Registrierungsprozess und progressiver Profilerstellung. CIAM hilft Unternehmen ebenfalls dabei, Vertrauen und Loyalität aufzubauen, da Verbraucher ihre Passwörter und Datenschutzeinstellungen einfach selbst verwalten können. Mit Enterprise CIAM können Unternehmen ferner Dienstleistungen mit hohem Mehrwert für ihre Kunden entwickeln, indem sie auf sichere Weise an dynamischen digitalen Partner-Ökosystemen teilnehmen. All dies führt zu **schnelleren Konversionsraten, höheren Bindungsraten und größerer Kundenloyalität**.

2. Großartige Erlebnisse

Im Rahmen ihrer Erneuerungsstrategie können Unternehmen CIAM nutzen, um unterschiedliche hybride Umgebungen im gesamten Unternehmen zu konsolidieren. Einer der vielen Vorteile davon ist eine einheitliche Sicht auf den Kunden, dank der Unternehmen ihre Omnichannel- und phygitalen User Journeys anpassen und personalisieren können, um großartige Erlebnisse bereitzustellen. Enterprise CIAM erlaubt es Unternehmen außerdem, das Internet der Dinge sicher in ihre Angebote zu integrieren und an digitalen Ökosystemen mit mehreren Partnern teilzunehmen, um ihren Kunden die gewünschten einfachen und komfortablen Erlebnisse zu bieten. Ferner kann die Lösung je nach Nutzung und Nachfrage problemlos skaliert werden, ohne dass es zu Unterbrechungen für die Kunden kommt. Diese und weitere Vorteile führen zu einem **höheren Omnichannel-Umsatz, einer geringeren Kundenabwanderung und einer besseren langfristigen Rentabilität**.

3. Höhere Kundensicherheit

Die wirtschaftliche Erneuerung erfordert die Einführung einer Vielzahl neuer Technologien und die Erprobung neuer Ansätze, wie z. B. die Teilnahme an digitalen Partner-Ökosystemen oder die Integration des Internet der Dinge in Produkte und Dienstleistungen. Enterprise CIAM wurde eigens für die Sicherheit von Verbrauchern, IoT und Unternehmen entwickelt und ermöglicht es Unternehmen, neue Lösungen auf sichere Weise in ihre Geschäftsstrategien und IT-Umgebungen zu integrieren. Damit dies möglich ist, unterstützt Enterprise CIAM moderne Sicherheitsmodelle, wie z. B. Zero Trust und CARTA, die auf der Annahme beruhen, dass keine Person bzw. kein Ding vertrauenswürdig ist und daher laufend überprüft werden muss. Enterprise CIAM ist auch der Schlüssel zur Einhaltung von Datenschutz-, Zustimmungs- und anderen gesetzlichen Bestimmungen Es bietet Kunden ein einfach zu bedienendes Dashboard, über das sie ihre Datenschutz- und Datenfreigabeeinstellungen selbst steuern können. All dies hilft Unternehmen bei der **Einhaltung von Datenschutzbestimmungen und der Minimierung von Risiken und Betrugsfällen**.

> „Im April 2020 haben wir BBC Bitesize eingeführt, eine Webseite, die Eltern und Schülern kostenlose Videos, Anleitungen, Aktivitäten und Ratespiele nach Themen und Klassenstufe sortiert anbietet. Das Relaunch hat nur wenige Wochen gedauert, und bereits am Einführungstag wurde der Service ohne Ausfall von drei Millionen Menschen genutzt."
>
> Matt Grest, Director of Platform
>
> BBC

ForgeRock: Der unangefochtene Marktführer für Enterprise CIAM

Als unangefochtener CIAM-Marktführer hilft ForgeRock Unternehmen , die acht Digitalisierungstrends erfolgreich aufzugreifen. Optimieren Sie Ihre Geschäftsabläufe mit ForgeRock und der branchenweit einzigen KI-basierten All-in-One-Plattform der Unternehmensklasse für alle Identitäten und jede Cloud.

Internationale Konzerne vertrauen auf ForgeRock CIAM, um Wachstum und Umsatz zu steigern. Werden Sie Mitglied der ForgeRock-Community und profitieren Sie von der Unterstützung Ihrer einzigartigen Initiativen, um nicht nur die Trends von heute, sondern auch die von morgen zu bedienen.

„Wir bei Philips haben es uns zur Aufgabe gemacht, das Leben der Menschen zu verbessern und sie zu befähigen, besser für sich und andere zu sorgen. Dank ForgeRock können wir innovative Technologien für Datenfreigabe- und Zustimmungsprozesse in unsere digitale HealthSuite-Plattform integrieren und so das Vertrauen von Verbrauchern und Patienten stärken.“

Jereon Tas, Chief Innovation and Strategy Officer

PHILIPS

Weitere Informationen

Mehr zu ForgeRock und CIAM

- **Schauen** Sie das ForgeRock CIAM-Einführungsvideo.
- **Lesen** Sie, wie die BBC personalisierte Inhalte für über 45 Millionen Nutzer weltweit liefert.
- **Laden** Sie unseren CIAM-Kaufleitfaden mit Informationen zu den wichtigsten Funktionen, Definitionen und Fragen an Anbieter herunter.

Jetzt ist es an der Zeit, in die Cloud zu migrieren, KI zu nutzen und die Vorteile von Infrastruktur der nächsten Generation zu erschließen; die Architektur, die Unternehmen heute aufbauen, bestimmt ihre Zukunft.[46]

accenture

Informationen von unabhängigen Dritten

Sehen Sie sich die Punktplatzierung an und lesen Sie in diesen Analystenberichten, warum ForgeRock der Enterprise CIAM-Marktführer ist:

- **The Forrester Wave™:** Customer Identity and Access Management, 2020
- **Gartner®** Critical Capabilities for Access Management, 2021
- **KuppingerCole Leadership Compass:** CIAM Platforms, 2020

- Schulung und Beratung zu CIAM-Markt und -Technologie erhalten Sie bei **The Cyber Hut**.

46 https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Full-Report.pdf

Über ForgeRock

ForgeRock®, (NYSE: FORG) ist ein weltweit führender Anbieter im Bereich digitale Identität. Das Unternehmen liefert moderne und umfassende Identity und Access Management-Lösungen für Verbraucher, Mitarbeiter und Dinge und bietet so einen einfachen und sicheren Zugang zur vernetzten Welt. Mit ForgeRock orchestrieren, verwalten und sichern mehr als 1.300 globale Unternehmen den gesamten Lebenszyklus von Identitäten, angefangen bei dynamischen Zugriffskontrollen, Governance und APIs bis hin zur Speicherung autoritativer Daten – verwendbar in jeder Cloud- oder Hybridumgebung. Das Unternehmen mit Hauptsitz in San Francisco, Kalifornien, unterhält Niederlassungen auf der ganzen Welt. Für weiterführende Information und kostenlose Downloads besuchen Sie gerne unsere Website **www.forgerock.com**.

Folgen Sie uns

ForgeRock