Aangeboden door:

okta

Customer Identity

for dummies®

A Wiley Brand

Waarom Customer Identity relevant is

Wat moderne Customer Identity voor u kan betekenen

Best practices op het gebied van Customer Identity

Lawrence C. Miller

Jeremie Certes

Speciale Okta-editie

Over Okta

Okta is de grootste Identity Company. We streven ernaar dat iedereen op veilige wijze elke mogelijke technologie kan gebruiken, op elke plek, op elk device en in elke app. Onze Workforce en Customer Identity Clouds bieden goed beveiligde maar toch flexibele toegang, authenticatie en automatisering om de manier te transformeren waarop mensen zich gedragen in de digitale wereld. Ze zorgen ervoor dat Identity een centrale rol speelt in de security en groei van organisaties.

Customer Identity

Speciale Okta-editie

door Lawrence C. Miller en Jeremie Certes

for dummies®
A Wiley Brand

Customer Identity voor Dummies®, speciale Okta-editie

Uitgegeven door
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-22817-1 (pbk); ISBN 978-1-394-22818-8 (ebk)

Colofon

Dit zijn enkele van de personen die hebben geholpen om dit boek op de markt te brengen:

Project-editor: Rachael Chilvers

Acquisitie-editor: Traci Martin

Redactioneel manager: Rev Mengle

Bedrijfsontwikkelaar: Molly Daughty

Productie-editor: Saikarthick Kumarasamy

Inleiding

Buiten uw werk bent u als particuliere klant van andere organisaties ongetwijfeld al weleens - bewust of onbewust - in aanraking gekomen met Customer Identity. Misschien toen u inlogde bij een website om tickets voor een concert te kopen. Of toen u uw social media-account gebruikte om in te loggen bij een nieuwe e-commercesite. Het kan ook zijn dat u uw mobiele telefoon gebruikt om te internetbankieren of dat u weleens eenmalige inlogcodes ontvangt via sms. Dit zijn een paar alledaagse voorbeelden van manieren waarop klanten Customer Identity al gebruiken voor allerlei applicaties, websites en portals.

In dit boek leggen we uit hoe moderne Customer Identity uw organisatie kan helpen een veilige, soepele customer experience te creëren voor elke gebruiker.

Over dit boek

Customer Identity voor Dummies, speciale Okta-editie, bestaat uit de volgende acht hoofdstukken:

- De basisbeginselen van Customer Identity (hoofdstuk 1)
- Waarom Customer Identity belangrijker is dan ooit (hoofdstuk 2)
- Waarom u niet moet proberen zelf een Customer Identity-oplossing te ontwikkelen (hoofdstuk 3)
- Wat een moderne Customer Identity-oplossing is en wat uw organisatie eraan heeft (hoofdstuk 4)
- Waar u op moet letten in de zoektocht naar een moderne Customer Identity-oplossing voor uw organisatie (hoofdstuk 5)
- Hoe uw organisatie succes boekt met een Customer Identity-oplossing om maat (hoofdstuk 6)
- De toekomst van Customer Identity (hoofdstuk 7)
- Tien belangrijke overwegingen om optimaal te presteren met een Customer Identity-oplossing (hoofdstuk 8)

Elk hoofdstuk van dit boek staat op zichzelf. Als een bepaald onderwerp u interessant lijkt, kunt u dus gewoon eerst dat hoofdstuk lezen. Met andere woorden, u kunt dit boek in elke gewenste volgorde lezen (maar misschien beter niet ondersteboven of achterstevoren).

Enkele aannames

Aannames zijn niet altijd nuttig, maar bij het schrijven van dit boek hebben we toch een paar aannames over u gedaan.

Voornamelijk dat u ergens werkt waar u verantwoordelijk bent voor het bouwen, schalen, moderniseren, integreren, ontwerpen en/of beveiligen van een applicatie, website of portal voor klanten en/of partners. Dan denken we bijvoorbeeld aan een applicatiedeveloper, applicatie-architect, productmanager, engineering-manager, digitale manager, CTO (chief technology officer), CIO (chief information officer), CPO (chief product officer), CISO (chief information security officer), CMO (chief marketing officer) of iemand die gespecialiseerd is in of vertrouwd is met Customer Iidentity.

Pictogrammen die in dit boek worden gebruikt

In dit boek gebruiken we speciale pictogrammen om de aandacht te vestigen op belangrijke informatie. Dit kunt u verwachten:

Dit pictogram wijst op belangrijke informatie die u in uw eigen langetermijngeheugen zou moeten opslaan.

Als technisch jargon u ook weleens boven de pet gaat, let dan op dit pictogram. U vindt hier een heldere uitleg van het gebruikte jargon.

Tips zijn altijd welkom, toch? Wij zijn er in elk geval van overtuigd dat u deze juweeltjes van informatie op prijs zult stellen.

Laat u niet afschrikken door onze waarschuwingen, want het zijn eigenlijk alleen maar goedbedoelde adviezen.

Buiten het boek

We kunnen helaas niet alles behandelen in dit beknopte boek, maar u kunt nog veel meer informatie vinden op `https://okta.com/customer-identity`.

IN DIT HOOFDSTUK

- **Definitie van Customer Identity and Access Management**
- **Slechte Customer Identity-experiences en de gevolgen voor klanten Experience**
- **Goede Customer Identity-user experiences voor mobiele apps, websites en portals**
- **De belangrijkste capabilities van Customer Identity**

Hoofdstuk 1

Wat is Customer Identity?

Gebruikersnamen en wachtwoorden zijn onderdeel van het normale dagelijkse leven geworden. Consumenten beheren verschillende accounts voor online winkels, bankrekeningen en mobiele apps. Dat is Customer Identity and Access Management (CIAM). U kunt aan de hand van uw eigen digitale experiences vast enkele verschillen tussen goede en slechte CIAM aanwijzen. De app voor mobiel bankieren geeft u waarschijnlijk een sterk gevoel van veiligheid en is gemakkelijk in het gebruik dankzij de eenvoudige authenticatie met een vingerafdruk of gezichtsscan. Daar staat tegenover dat u vast ook weleens een online winkelwagentje heeft achtergelaten toen u een ellenlang registratieformulier moest invullen. Soms neemt de registratie zelfs meer tijd in beslag dan het vinden van de producten die u wilt kopen!

In dit hoofdstuk behandelen we de basisbeginselen van Customer Identity. Wat is het, waarom heeft een slechte Customer Identity-experience een negatief effect op klanten, waarom heeft u Customer Identity nodig voor uw klanten en applicaties

en wat zijn de belangrijkste capabilities die elke Customer Identity-oplossing moet bieden?

Customer Identity uitgelegd

Misschien klinkt Customer Identity u niet bekend in de oren, maar het is wel een wezenlijk onderdeel van uw dagelijkse leven. Bijvoorbeeld wanneer u een app op uw mobiele telefoon opent, u registreert voor een nieuwe online service of u aanmeldt bij uw favoriete website. Customer Identity voegt een digitale identity-laag toe die kan worden geïntegreerd in uw klantgerichte apps, websites en portals. Met Customer Identity kunt u zien wie uw klanten zijn, welk device ze meestal gebruiken, tot welke onderdelen van uw klantgerichte services (apps, portals en websites) ze toegang hebben en waar ter wereld ze zich bevinden. Customer Identity omvat dus niet alleen de aanmelding van de gebruiker maar ook alles wat met de registratie samenhangt.

Met een slechte Customer Identity-experience jaagt u uw klanten naar de concurrent die een meer intuïtieve customer experience (CX) met minder frictie biedt. Maar wat is nu precies een slechte Customer Identity-experience?

Goede en slechte Customer Identity vergelijken

De beveiliging van de toegang en de data van de klant is van cruciaal belang bij de customer experiences die u biedt. Maar een veilige toegang is niets waard als de CX zo moeilijk en frustrerend is dat de klant het te ingewikkeld vindt om met u te communiceren. U heeft vast zelf ook weleens een slechte Customer Identity-experience gehad bij een persoonlijke of zakelijke transactie. Hieronder hebben we enkele voorbeelden van veel voorkomende knelpunten voor u op een rijtje gezet:

- Een account en een wachtwoord moeten aanmaken alleen maar om een website te kunnen bekijken.
- Een nieuw account en een nieuw wachtwoord moeten aanmaken voor elke afzonderlijke app, website en portal van dezelfde organisatie.

- Inloggen met verschillende accounts en wachtwoorden om toegang te krijgen tot verschillende services van dezelfde organisatie.
- Bij de registratie bijna uw hele levensverhaal moeten vertellen alleen maar om een account aan te maken.
- Op een ander device ineens een andere login-experience en andere functionaliteiten voorgeschoteld krijgen.
- De klantenservice moeten bellen om een vergeten of verkeerd wachtwoord te resetten.
- Bij het inloggen iedere keer naast een wachtwoord ook een sms-code moeten invullen, zelfs als u altijd vanaf dezelfde locatie en hetzelfde device inlogt.

Een goede Customer Identity-experience ziet er daarentegen zo uit:

- Eenvoudige registratie en met een minimale hoeveelheid gegevens een account kunnen aanmaken om meteen aan de slag te gaan.
- Gezichtsherkenning op een smart device (geen wachtwoord nodig).
- Verificatie met sms of e-mail om een vertrouwelijke financiële transactie extra te beveiligen.
- Met hetzelfde account toegang kunnen krijgen tot alle services van een organisatie.

Een slechte Customer Identity-experience voegt veel onnodige frictie aan de customer journey toe. Bijvoorbeeld door gebruikers een ellenlang registratieformulier te laten invullen of ze te dwingen contact met het callcenter op te nemen om een wachtwoord te resetten. Slechte Customer Identity heeft ook tot gevolg dat uw developers speciale integraties en connecties voor nieuwe apps moeten bouwen, waardoor de time-to-market langer duurt. Vaak moeten klanten ook afzonderlijke gebruikersaccounts aanmaken voor elke app, website en portal in de digitale omgeving van een organisatie. De admins moeten al deze accounts vervolgens in afzonderlijke directory's beheren. Tot slot biedt slechte Customer Identity niet de betrouwbaarheid en schaalbaarheid die flexibele organisaties nodig hebben in de digitale economie.


TIP

Zorg dat uw Customer Identity-contactmomenten geen pijnpunten worden voor klanten. Customer Identity moet de start zijn van een prettige CX die de hele customer journey blijft voortduren.

Soorten klanten, bedrijfsmodellen en applicaties

U heeft een moderne Customer Identity-oplossing nodig om 24x7x365 een frictieloze omnichannel-CX te bieden voor al uw producten en services, ongeacht waar uw klanten contact leggen met uw organisatie. Customer Identity is de eerste stap in de customer journey voor veel apps, websites en portals en is om die reden essentieel voor de hele customer services experience.

Uw organisatie doet mogelijk zaken met particuliere consumenten, met andere organisaties of met beide. Een Customer Identity-oplossing moet zowel deze verschillende typen klanten als een verscheidenheid aan bedrijfsmodellen ondersteunen, waaronder business-to-consumer (B2C), business-to-business (B2B) en business-to-business-to-consumer (B2B2C).

Het kan zijn dat uw verschillende typen klanten het liefst via een bepaald kanaal zaken met uw organisatie doen. Zo gebruiken particuliere consumenten meestal uw mobiele app, terwijl zakenpartners liever via hun werkcomputer met uw organisatie communiceren. Customer Identity moet al deze verschillende typen klanten ondersteunen, welke kanalen en devices ze ook gebruiken.

Voor de ondersteuning van B2B- en B2B2C-bedrijfsmodellen moet u wellicht veilige connecties en integraties met de apps en portals van uw partners implementeren. Mogelijk moet u ook identities van uw partners samenvoegen of bundelen met behulp van enterprise directory-services, zoals Active Directory en Lightweight Directory Access Protocol (LDAP).

Tot slot moeten klanten uw services kunnen gebruiken via alle mobiele apps, websites en portals. De customer experience moet naast frictieloos ook voor alle typen applicaties consistent zijn en dezelfde functionaliteit bieden.

Belangrijkste capabilities

De drie belangrijkste capabilities van een effectieve Customer Identity-oplossing zijn authenticatie, autorisatie en user management. In Customer Identity bestaan uw gebruikers uit klanten en partners.

Een goede authenticatie controleert of de mensen die inloggen bij hun account daadwerkelijk zijn wie ze beweren te zijn. Zo wordt voorkomen dat kwaadwillenden toegang krijgen tot gevoelige gebruikersdata (zoals betalingsgegevens, adressen en burgerservicenummers) of dat ze frauduleuze transacties uitvoeren (zoals geld van een bankrekening overschrijven).

Een effectieve autorisatie controleert of een gebruiker het juiste toegangsniveau tot bepaalde applicaties en/of resource heeft.

Een duidelijk user management biedt admins de mogelijkheid om de toegangsrechten van gebruikers bij te werken en security-policies te implementeren, zodat ze frictieloze en veilige experiences kunnen blijven aanbieden, en vertrouwen kunnen opbouwen bij elke klant.

IN DIT HOOFDSTUK

- **De vraag naar superieure customer experiences**
- **Vertrouwen als hoeksteen van klantrelaties**
- **Ondersteuning en bevordering van de digitale transformatie**

Hoofdstuk 2

Waarom Customer Identity nu belangrijker is dan ooit tevoren

Klanten verwachten en eisen vandaag de dag een moderne, frictieloze, gepersonaliseerde customer experience (CX) bij elke interactie met uw organisatie. Organisaties die dat niet kunnen bieden, slagen er niet in om nieuwe klanten aan te trekken en bestaande klanten vast te houden.

Het scheppen van vertrouwen is ook absoluut cruciaal. Organisaties die de security en privacy van persoonsgegevens niet goed op orde hebben, raken klanten kwijt, óók klanten die niet direct zijn getroffen door een datalek, maar als gevolg daarvan het vertrouwen in de organisatie hebben verloren.

Tot slot is digitale transformatie niet langer een vrijblijvend initiatief meer, maar een verplichting geworden. Elke organisatie, in welke sector ook, moet zich omvormen tot een technologie-organisatie om te kunnen overleven en met succes te kunnen opereren in de moderne digitale economie.

In dit hoofdstuk leggen we uit hoe de vereisten op het gebied van customer experience, security, privacy en digitale transformatie

de behoefte aan een moderne Customer Identity-oplossing niet alleen ondersteunen, maar ook steeds groter en urgenter maken. Nu meer dan ooit tevoren.

Inspelen op de vraag naar moderne customer experiences

De moderne CX is frictieloos, gepersonaliseerd en omnichannel. Uw klanten willen 24x7x365 snel en frictieloos toegang hebben tot producten, services, informatie en andere resources op het device waaraan ze de voorkeur geven, of dit nu een smart device, computer, tablet of smartphone is.

Nog niet zo lang geleden kochten mensen bijna al hun spullen in een fysieke winkel en bekeken ze films in de bioscoop of op de dag en tijd dat ze op tv werden uitgezonden. Toen mensen steeds meer via hun eigen computer met organisaties in contact kwamen, werd het ook steeds belangrijker dat websites een prettige user experience boden. Tegenwoordig gebruiken mensen hun smartphone om boodschappen te bestellen die vervolgens bij de voordeur worden afgeleverd terwijl ze aan het werk zijn. En ze kunnen hun favoriete tv-programma's op elk moment, op elke locatie en op elk device bekijken. Organisaties zoals Amazon en Netflix stellen de norm voor frictieloze CX in alle kanalen, met als gevolg dat consumenten dezelfde kwaliteit verwachten van elke organisatie met wie ze zaken doen, ook úw organisatie. Daarom is het nu belangrijker dan ooit tevoren om uw klanten een moderne access experience te bieden.


WAARSCHUWING

Volgens PwC (rapport: The Future of Customer Experience, 2018) zegt 32 procent van de klanten een favoriet merk vaarwel na slechts één slechte ervaring en doet 59 procent dit na twee slechte ervaringen. Ook uw klanten zullen geen genoegen nemen met een trage, omslachtige login-experience waar geen eind aan lijkt te komen.

Organisaties hebben een moderne Customer Identity-oplossing nodig om een superieure customer service experience te creëren die het volgende biedt:

- **Uniforme digitale experiences op alle devices:** klanten vinden het niet leuk als ze meerdere keren moeten registreren of inloggen bij verschillende services van dezelfde organisatie. Ze willen een consistente en volledig functionele experience, of ze nu uw website openen op hun computer of op hun mobiele device, en ongeacht welke van uw mobiele apps ze gebruiken. Dat betekent dat u 24x7x365 een frictieloze, veilige login in uw eigen huisstijl moet bieden, op elk device en op elke locatie ter wereld.
- **Gepersonaliseerde customer journeys:** als u in al uw kanalen uit de eerste hand betrouwbare informatie verzamelt over voorkeuren (waaronder toestemmingen), kunt u makkelijker een 360-graden beeld van uw klanten opbouwen. Vervolgens kunt u deze identities en profielen van klanten consolideren op één plek en de customer journey afstemmen op individuele voorkeuren. Als consumenten het gevoel hebben dat u ze begrijpt, is de kans ook groter dat ze zaken met u willen doen en hun positieve ervaringen met anderen willen delen.
- **Nieuwe en moderne experiences:** de technologie ontwikkelt zich razendsnel, stuurt verwachtingen van klanten een bepaalde richting uit en staat aan de wieg van nieuwe trends. Tien jaar geleden gebruikten klanten hun smartphone alleen om te bellen en hun e-mail te checken. Vandaag kunnen klanten een belangrijk onderdeel bestellen via de app van uw organisatie die op hun smartphone is geïnstalleerd terwijl ze met de bus of trein naar hun werk gaan. En ze verwachten dat het de volgende dag wordt geleverd. Met een moderne Customer Identity-oplossing kunt u uw klanten een frictieloze experience bieden met innovaties die op alle devices kunnen worden gebruikt, zoals passwordless authenticatie (bijvoorbeeld via gezichtsherkenning en vingerafdrukidentificatie).


HERINNERING

Oplossingen voor workforce identity en customer identity zijn allebei cruciale technologieën in de tech stack van een organisatie. Uw werknemers zullen uw organisatie niet zo snel de rug toekeren vanwege een slechte inlog-experience, maar uw klanten stappen zonder meer over naar de concurrent als u geen superieure end-to-end CX met een frictieloos, gepersonaliseerd omnichannel login-proces biedt.

Een vertrouwensrelatie opbouwen met elke klant

Het opbouwen van het vertrouwen van de klant is cruciaal voor het succes van elke organisatie. Helaas worden de persoons- en accountgegevens die klanten aan organisaties toevertrouwen voortdurend en van alle kanten bedreigd. En veel te vaak wordt het vertrouwen van de klant beschaamd. Daarom moet het beschermen van de accounts en gegevens van klanten een topprioriteit zijn. Als uw klanten geen vertrouwen in u hebben, bent u ze in een mum van tijd kwijt.

Klanten die een slechte ervaring hebben met uw organisatie of het vertrouwen in uw organisatie verliezen, houden dat niet voor zichzelf. Met dank aan de social media!

Moderne cyberbedreigingen en -aanvallen zijn geraffineerder, vernietigender, frequenter en massaler dan ooit tevoren. De wereldwijde coronapandemie heeft de cybercriminaliteit niet afgeremd. Integendeel, in de eerste helft van 2020 zijn bijna 16 miljard gegevensrecords uitgelekt; dat is een stijging van 273 procent ten opzichte van de eerste helft van 2019, zo blijkt uit gegevens van Security Boulevard (https://securityboulevard.com).

Het is een niet te ontkennen feit dat een datalek consumenten in financieel en persoonlijk opzicht op de rand van de afgrond kan brengen. Het kan jaren duren voordat iemand een financieel verlies of een identiteitsdiefstal weer te boven is. En velen lukt dat nooit.

Voor organisaties kan de financiële schade makkelijk tientallen of honderden miljoenen dollars bedragen. In 2018 maakte hotelketen Marriott International bekend dat aanvallers de data van meer dan 380 miljoen gasten hadden gestolen. Het datalek kostte Marriott ruim 44 miljoen dollar alleen al in het eerste kwartaal nadat het lek aan het licht kwam. Daarna kreeg de organisatie nog een boete van 25 miljoen dollar van de ICO (Information Commissioner's Office) in het VK. Maar het verlies aan omzet als gevolg van reputatieschade en het verlies van klantvertrouwen is waarschijnlijk nog veel groter. Veel organisaties slagen er nooit

meer in het verlies van klantvertrouwen als gevolg van uitgelekte data en accounts terug te winnen (als ze al blijven bestaan).

Een moderne Customer Identity-oplossing kan organisaties als volgt helpen bij het opbouwen en behouden van klantvertrouwen:

- **Klantenaccounts beveiligen:** cyberaanvallen worden steeds geraffineerder en vernietigender. Wachtwoorden zijn niet meer voldoende om de accounts van uw klanten te beschermen. Bovendien heeft bijna iedereen een hekel aan wachtwoorden. Bescherm de Customer Identity-lifecycle in al uw apps door uw klanten tijdens de registratie, de authenticatie en de in-app activiteiten te beschermen met multi-factor authenticatie en passwordless authenticatie.
- **Privacy en toestemmingen beheren:** klanten verwachten dat de security en privacy van hun persoonsgegevens is gewaarborgd. Het fundamentele recht op privacy is nu vastgelegd in een groot aantal wetten, waaronder de AVG (Algemene verordening gegevensbescherming) en de CCPA (California Consumer Privacy Act). Uw Customer Identity-oplossing moet een frictieloze en intuïtieve CX bieden en klanten zelf laten bepalen welke persoonsgegevens uw organisatie mag gebruiken, delen en opslaan. Als het identity-platform van uw organisatie de nieuwste wet- en regelgeving niet kan ondersteunen, liggen juridische problemen op de loer.
- **Wettelijke verplichtingen naleven:** de AVG en CCPA zijn maar twee voorbeelden van de tientallen strikte security- en privacywetten die in de afgelopen paar jaar wereldwijd zijn ingevoerd. Deze trend zal zich onvermijdelijk voortzetten in de nabije toekomst. De CCPA was bijvoorbeeld nog niet eens een heel jaar van kracht toen de CPRA (California Privacy Rights Act) werd aangenomen in november 2020. Organisaties die zich niet aan de toepasselijke wet- en regelgeving houden, kunnen financiële schade oplopen als gevolg van negatieve auditresultaten en/of het gedwongen moeten staken van alle activiteiten.

Digitale transformatie versnellen

Vandaag de dag moet elke organisatie zich tot een technologie-organisatie omvormen om te kunnen overleven en met succes te kunnen opereren. Elke sector krijgt te maken met digitale transformatie en deze trend breidt zich nu sneller uit dan ooit tevoren. Videotheken (en zelfs bioscopen) zijn bijvoorbeeld kopje onder gegaan in het kielzog van streaming media-services, en taxibedrijven worstelen met concurrerende services voor het delen van autoritten. Veel organisaties worden echter ook geconfronteerd met grote technische schulden op het moment dat ze afscheid willen nemen van hun omslachtige legacy systemen. Voor een soepele digitale transformatie moeten organisaties hun technische infrastructuur moderniseren en naar de API-economie (application programming interface) overschakelen.

Technische schulden zijn de impliciete kosten van werk dat opnieuw gedaan moet worden als gevolg van een eerdere beslissing om in plaats van de juiste oplossing een eenvoudigere oplossing te implementeren.

Organisaties hebben om de volgende redenen een moderne Customer Identity-oplossing nodig voor het ondersteunen en versnellen van de digitale transformatie:

- **De overstap naar de cloud:** voor de meeste organisaties vormt de cloud een integraal onderdeel van hun strategie voor digitale transformatie. Vooral omdat legacy infrastructuur een remmende werking heeft op de flexibiliteit en het vermogen van een organisatie om een moderne customer experience te bieden. Het kan echter jaren duren voordat een organisatie de overstap naar de cloud heeft voltooid. Maar met één identity-laag die zowel voor legacy on-prem apps als voor moderne web-apps en mobiele apps kan worden gebruikt, vereenvoudigt u het beheer van hybride cloudomgevingen die zijn opgebouwd uit openbare clouds, persoonlijke clouds en on-prem resources. Hieronder hebben we een aantal voordelen van de cloud op een rijtje gezet.
  - *Verbeterde development van apps, meer flexibiliteit bij implementaties en lagere kosten:* organisaties kunnen cloudservices en resources snel implementeren

en on-demand opschalen, zodat legacy identity-infrastructuren kunnen worden afgeschaft en ook de hoge kosten voor het onderhoud kunnen worden geschrapt.

- *Gebruik van microservices-architectuur en API's:* softwaredevelopers bouwen apps tegenwoordig met behulp van microservices en API's. Dergelijke architecturen vereisen een holistische en gecentraliseerde benadering van identity om uw klanten en partners veilig toegang te bieden. Met een moderne Customer Identity-oplossing in de cloud kunnen uw developers snel en eenvoudig opties voor authenticatie, autorisatie en user management in nieuwe apps integreren, zodat ze meer tijd overhouden om zich op de primaire activiteiten van de organisatie te richten.

  Microservices zijn kleine, op zichzelf staande services die onafhankelijk kunnen worden geïmplementeerd en losjes aan elkaar kunnen worden gekoppeld om op die manier de individuele componenten van een applicatie te leveren. Een API (application programming interface) biedt applicaties de mogelijkheid om met elkaar te communiceren via een softwareconnectie.


VAKTAAL

» **Deelname aan de API-economie:** API's zijn niet langer slechts een developmenttechniek, maar de drijvende kracht achter een nieuw bedrijfsmodel waarmee organisaties inkomsten uit de toegang tot hun eigen API's kunnen genereren. Denk bijvoorbeeld aan een kaartoverlay in een taxiservice-app of een beveiligd afrekenproces via een social media-account voor een maaltijdbezorgingsapp. Een moderne Customer Identity-oplossing kan de toegang tot API's beheren en beveiligen, zodat organisaties hun API-gedreven organisatie kunnen uitbreiden en opschalen.

IN DIT HOOFDSTUK

- **Het bouwen van frictieloze en veilige customer experiences**
- **Schaarse developers en de focus op primaire taken**
- **Betrouwbaarheid op elke schaal, integratie met de tech stack en snellere time-to-market**
- **De volledige kosten van bouwen versus kopen**

Hoofdstuk **3**

Customer Identity ontwikkelen

In hoofdstuk 2 hebben we het gehad over waarom een moderne Customer Identity-oplossing van cruciaal belang is om een superieure customer experience (CX) te bieden, vertrouwen bij de klant op te bouwen en de digitale transformatie te versnellen. Misschien denkt u op dit moment wel: "Dat gaan we zelf wel even doen". Maar het bouwen van een eigen Customer Identity-oplossing is moeilijker dan u denkt. In dit hoofdstuk leggen we uit waarom.

Customer experience versus security en compliance: een delicaat evenwicht

Als u een customer Identity-oplossing bouwt, moet u twee tegenstelde belangen zorgvuldig met elkaar in evenwicht brengen: het leveren van een superieure CX en het bieden van security en compliance.

Bedenk maar eens wat de kenmerken van een superieure customer experience zijn. Per slot van rekening heeft u in uw dagelijkse leven ook vaak genoeg interacties met andere organisaties. Waar wordt u blij van als online klant? Wellicht heeft uw ideale customer experience de volgende kenmerken:

- **Een frictieloos registratieproces:** de registratie moet eenvoudig en snel verlopen de eerste keer dat u een website bezoekt of een app gebruikt. Misschien wordt u gevraagd een klein beetje relevante informatie op te geven tijdens uw eerste bezoek en uw volgende bezoeken, maar u hoeft niet uw hele levensverhaal te vertellen zodra u de virtuele deur opendoet. Dit wordt progressive profiling genoemd.
- **Een intuïtief en frictieloos loginproces:** bij het inloggen moeten verschillende authenticatiemethoden worden aangeboden die op uw individuele voorkeuren zijn afgestemd. De meeste mensen hebben een hekel aan wachtwoorden. Dus alles waarvoor ze geen wachtwoord hoeven aan te maken en te onthouden is ideaal, bijvoorbeeld inloggen via een bestaand social media-account of door middel van gezichtsherkenning.
- **Single sign-on voor alle apps van dezelfde organisatie:** een klantenportal moet met één login-experience naadloos toegang tot alle gewenste apps bieden.
- **Een customer experience in de vertrouwde huisstijl:** u moet onmiddellijk de merken zien die u herkent en vertrouwt, ook als u verschillende apps of services gebruikt die door dezelfde organisatie worden geleverd (bijvoorbeeld Amazon Prime Video en Whole Foods die beide via dezelfde Amazon-website toegankelijk zijn).
- **Alle kanalen, in uw voorkeurstaal:** een consistente login-experience op elk device, op elk moment, op elke locatie ter wereld en in de taal waaraan u de voorkeur geeft.
- **Gepersonaliseerde aanbevelingen:** relevante aanbevelingen voor producten en services die gebaseerd zijn op uw profielgegevens en aankoopgeschiedenis.

Om een superieure customer experience te kunnen ontwikkelen in een eigen Customer Identity-oplossing, moet u eerst bepalen wat de wensen van uw klanten zijn. En die kunnen sterk uiteenlopen. Bovendien vinden niet alle klanten hetzelfde belangrijk. Wat sommigen erg prettig vinden, brengt anderen in verwarring.

CUSTOMER IDENTITY IS OOK BELANGRIJK VOOR B2B

Hoewel dit hoofdstuk is gericht op de B2C-customer experience (business-to-consumer), moeten B2B-apps (business-to-business) ook een frictieloze en intuïtieve customer experience bieden. In veel B2B-relaties is de ene organisatie immers vaak de leverancier en de andere de klant. Veel Customer Identity-vereisten voor B2B zijn dus gelijk aan die voor B2C. Maar B2B-gebruikers kunnen specifieke, aanvullende wensen hebben, bijvoorbeeld de mogelijkheid om in te loggen op de website of app van een partner met de inloggegevens van hun organisatie, zonder dat een nieuw account hoeft te worden aangemaakt.

Het juiste evenwicht vinden tussen security en compliance enerzijds en een frictieloze customer service experience anderzijds is al een uitdaging op zichzelf.

Overweegt u toch om zelf een Customer Identity-oplossing te bouwen, houd dan rekening met de volgende risico's:

- **Het bouwen van een oplossing is gemakkelijker gezegd dan gedaan.** Het begint al met de security-methoden die uw klanten verwachten en nodig hebben. Denk bijvoorbeeld aan eenmalige wachtwoorden, passwordless authenticatie, multi-factor authenticatie en adaptive multi-factor authenticatie (waarbij alleen om extra factoren wordt gevraagd als dat gezien de risicoscore nodig is).
- **U moet voortdurend proberen cybercriminelen een stap voor te blijven.** Zelfs gespecialiseerde security-teams kunnen het tempo waarin ze bescherming moeten bieden tegen nieuwe exploits en kwetsbaarheden nauwelijks bijbenen. Geavanceerde cyberbedreigingen en -aanvallen maken steeds vaker gebruik van uitgelekte inloggegevens van online accounts. Als u een Customer Identity-oplossing bouwt, kunt u er dus op rekenen dat er hackers op afkomen. Voorheen waren gebruikers de zwakste schakel in de security van een organisatie. Zorg er dus voor dat uw

zelfgemaakte Customer Identity-oplossing niet de nieuwe zwakste schakel wordt.

- **De eisen van uw klanten blijven veranderen.** Vandaag willen ze geen wachtwoorden meer. Morgen vinden ze misschien dat het per sms ontvangen van toegangscodes op hun smartphone te veel gedoe is. Het bijhouden van de steeds veranderende verwachtingen van klanten is lastig. Als Customer Identity niet uw primaire activiteit is, moet u er dus ook rekening mee houden dat u constant veranderingen moet doorvoeren om uw klanten tevreden te houden.
- **De wet- en regelgeving op het gebied van compliance ondergaat een ware aardverschuiving.** De wetten en regels zijn eigenlijk constant aan verandering onderhevig en worden steeds complexer. Security- en privacywetten, zoals de AVG (Algemene verordening gegevensbescherming) en in de VS de HIPAA (Health Insurance Portability and Accountability Act) en de CCPA (California Consumer Privacy Act), zijn nog maar een paar van de ingewikkelde wetten met vaak conflicterende vereisten die aan de lopende band worden ingevoerd, bijgewerkt, vervangen en herzien. Als u een zelfgemaakte Customer Identity-oplossing gebruikt die niet aan de wettelijke vereisten voldoet, kan uw organisaties hoge boetes en andere sancties opgelegd krijgen.

Tot slot krijgt u bij het bouwen van uw eigen Customer Identity-oplossing ook met een aantal tegenstrijdige belangen te maken:

- **Security-innovatie gaat altijd door en u mag niet achterblijven.** Alle innovatieve functies die u wilt bouwen, zoals AMFA (adaptive multi-factor authenticatie), passwordless authenticatie, biometrische identificatie en eenmalige wachtwoorden, moeten toekomstbestendig zijn als u voorop wilt blijven lopen. Maar deze functies mogen geen extra frictie aan de customer experience toevoegen. Dat is het eerste tegenstrijdige belang omdat elke extra authenticatiefactor frictie toevoegt.
- **Verschillende mensen in uw organisatie hebben verschillende meningen en prioriteiten.** Het marketingteam wil een frictieloze en superieure user experience. Het salesteam kan niet langer wachten en wil alles 'gisteren' klaar hebben. Het security-team wil boven alles een extreem veilige toegang. De product- en

engineeringteams willen zich op het feitelijke product focussen in plaats van op de authenticatie. Het financiële team kiest uiteraard voor het hoogste rendement tegen de laagste investering. En uw CEO wil het allemaal!

Aan de ene kant willen organisaties een superieure customer service experience met een frictieloos en intuïtief registratie- en loginproces dat snel en eenvoudig toegang geeft tot uw applicaties. Aan de andere kant eisen klanten dat organisaties hun persoonsgegevens veilig en privé houden. Als uw klanten uw organisatie niet vertrouwen, gaan ze naar de concurrent. Voordat u besluit zelf een Customer Identity-oplossing te bouwen raden we u aan goed na te denken over alle uitdagingen die u moet overwinnen om het juiste evenwicht te vinden tussen een frictieloze CX aan de ene kant en robuuste security en compliance aan de andere kant. Bespreek dit vervolgens allemaal met uw developers (zie het volgende gedeelte).

Goede developers aantrekken en vasthouden

Oké, u heeft hele goede developers. Om precies te zijn, u heeft de allerbeste developers van de hele wereld. Daarom betaalt u ze ook zo'n hoog salaris, toch? Maar heeft u voldoende goede developers? Gezien het wereldwijde tekort aan goede developers, moeten de meeste organisaties veel moeite doen om toptalenten aan te trekken en vast te houden.

En van welke andere IT-professionals zijn er wereldwijd ook veel te weinig? Inderdaad, security-engineers. Als u een developer heeft die een veilige Customer Identity-oplossing kan ontwikkelen die niet alleen een superieure CX, maar ook robuuste security en privacy biedt en bovendien aan de voortdurend veranderende wet- en regelgeving voldoet, dan heeft u inderdaad een lot uit de loterij. Als identity and access management (IAM) niet uw core business is, waarom zou u Twilight Sparkle en Rainbow Dash (voor de niet-ingewijden: dit zijn eenhoorns uit *My Little Pony*) dan uw Customer Identity-oplossing laten bouwen? Zou het niet

beter zijn als zo'n groot talent zich voor de volle 100 procent zou kunnen focussen op uw kernactiviteit en de apps en websites waarmee uw inkomsten worden gegenereerd?

Het zelf bouwen van Customer Identity vereist heel veel maatwerkcode. Volgens de Top Tien van het *Open Web Application Security Project (OWASP)* (`https://owasp.org`) wordt 93 procent van alle kwetsbaarheden in apps ontdekt in maatwerkcode. Dergelijke kwetsbaarheden stellen uw organisatie en uw klanten bloot aan grote security-lekken en creëren hoge technische schulden en opportuniteitskosten. Volgens Stripe.com (`https://stripe.com/files/reports/the-developer-coefficient.pdf`) besteden developers daarnaast 42 procent van hun tijd aan het opsporen van fouten en het onderhouden van slechte legacy code in plaats van aan het bouwen van nieuwe apps. Het aantrekken en vasthouden van toptalenten is veel moeilijker als uw developers een groot deel van hun tijd moeten besteden aan het opsporen van bugs.

Aanvullende overwegingen

Het is dus belangrijk om het juiste evenwicht te vinden tussen een frictieloze customer experience en robuuste security en effectieve compliance. Ook is het beter als getalenteerde developers zich volledig op hun kerntaken kunnen richten. Maar er zijn nog een aantal andere uitdagingen waaraan u moet denken voordat u besluit zelf uw eigen Customer Identity-oplossing te bouwen:

- **Betrouwbaarheid op grote schaal:** klanten verwachten frictieloze en veilige toegang tot uw mobiele apps, klantenwebsites en partnerportals op hun favoriete devices, vanaf elke locatie en 24x7x365, dus ook in perioden wanneer er een piek in de vraag is, bijvoorbeeld op Black Friday, als de belastingaangiften moeten worden gedaan, of tijdens de voorverkoop van tickets voor een populair concert, een groot sportevenement of een nieuwe film. Downtime leidt tot omzetverlies en reputatieschade van uw merk. Maar het ontwikkelen, bouwen en onderhouden van de infrastructuur

die nodig is om een betrouwbare service op grote schaal te ondersteunen, is complex en duur. Weet u zeker dat u uw eigen infrastructuur wilt beheren en problemen met storingen, onderbrekingen, onderhoudstaken en upgrades zelf wilt oplossen?

- **Integratie met uw tech stack:** uw Customer Identity-oplossing moet een veilige connectie tot stand brengen met de andere tools en applicaties in uw tech stack (zoals software voor het beheren van security, privacy, marketing en services) om alle mogelijkheden optimaal te benutten en de ROI te maximaliseren.
- **Snellere time-to-market:** organisaties moeten nieuwe, frictieloze en veilige CX snel invoeren om aan de steeds hogere verwachtingen van klanten te voldoen en in te spelen op de steeds grotere en complexere security- en compliancerisico's. U weet dat een Customer Identity-oplossing op maat die aan deze vereisten voldoet gecompliceerd en duur is. Maar wat als uw klanten geen sms'jes voor MFA meer willen gebruiken of als u aan wettelijke verplichtingen moet voldoen in een ander land waarnaar u wilt uitbreiden? De ontwikkeling van een Customer Identity-oplossing is een proces dat altijd doorloopt. Het is een eeuwigdurende cyclus die steeds weer innovaties en productontwikkelingen vereist om soepel te kunnen inspringen op voortdurend veranderende eisen van klanten en snel opkomende security-bedreigingen.

Dé beslissing: bouwen of kopen?

Het is bijzonder moeilijk om een Customer Identity-oplossing te bouwen die aansluit op de specifieke behoeften van uw klanten. Bovendien brengt het voortdurende onderhoud ook hoge kosten met zich mee. U moet een goed inzicht hebben in de eisen die uw klanten stellen aan een frictieloze maar veilige customer experience. Daarnaast moet u een team van zeer schaarse, heel bekwame, uitermate goed betaalde developers tot uw beschikking hebben om veilige code te schrijven en te onderhouden. Plus een zeer complexe, dure infrastructuur om 24x7x365 op grote schaal

toegang te kunnen garanderen. Tot slot moeten er integraties met uw hele tech stack worden gebouwd en is een snelle time-to-market noodzakelijk om nieuwe functionaliteiten in de belangrijkste apps van uw organisatie te implementeren.

Neem dus voordat u besluit zelf een Customer Identity-oplossing te bouwen de volledige kosten in ogenschouw, dus inclusief de technische schulden, het risico op security-lekken en de opportuniteitskosten.

Het bouwen van uw eigen Customer Identity-oplossing is gecompliceerd en in principe niet nodig. Maar neem in elk geval geen genoegen met een middelmatige oplossing! In hoofdstuk 4 leggen we uit wat de voordelen zijn van een moderne Customer Identity-oplossing en in hoofdstuk 5 leest u waar u op moet letten bij een moderne Customer Identity-oplossing.

IN DIT HOOFDSTUK

- De definitie van een moderne Customer Identity-oplossing
- Meer Customer Identity-mogelijkheden met een platformbenadering
- Moderne Customer Identity voor veilige, betrouwbare en schaalbare services
- Essentiële use cases en klantverhalen

Hoofdstuk **4**

De voordelen van een moderne Customer Identity-oplossing

Zoals uitgelegd in hoofdstuk 3 is het zelf bouwen van een Customer Identity-oplossing zeer ingewikkeld en erg duur. Het is voor organisaties daarom niet zinvol om hun schaarse app-developers van hun kerntaken af te houden door ze een Customer Identity-oplossing te laten ontwikkelen. In dit hoofdstuk leggen we uit waarom u beter kunt samenwerken met een expert die met een moderne Customer Identity-oplossing de knelpunten oplost en een frictieloze en veilige customer experience (CX) mogelijk maakt, zodat uw organisatie optimaal kan presteren.

Wat is een Customer Identity-oplossing?

Een moderne Customer Identity-oplossing voegt een digitale identity-laag toe die snel en soepel kan worden geïntegreerd in uw klantgerichte apps, websites en portals. Een dergelijke

oplossing helpt organisaties vertrouwen op te bouwen, biedt frictieloze customer experiences, een snelle time-to-market, security op internetschaal en een gecentraliseerd beheer van alle identities en access policies, zodat organisaties ruimschoots aan de verwachtingen van de klant kunnen voldoen.

Frictieloze user experiences

Als u frictieloze experiences wilt creëren, moet u uw klanten kennen en weten wat ze willen. Met een moderne Customer Identity-oplossing kunt u een 360-graden klantbeeld opbouwen dat op al uw apps en producten is gebaseerd, ongeacht waar, wanneer en op welk device de interacties met uw merk plaatsvinden. U kunt deze informatie als volgt gebruiken om experiences op maat te creëren en de frictie terug te dringen:

- Bied een uniforme en consistente customer experience voor al uw verschillende apps en websites, zonder uw gebruikers te vragen steeds opnieuw in te loggen.
- Vereis minder (of geen) wachtwoorden voor uw verschillende kanalen en de verschillende devices van uw klanten.
- Vraag prospects tijdens de registratie alleen om informatie die strikt noodzakelijk is.
- Sta uw zakenpartners toe om in te loggen met hun zakelijke inloggegevens, in plaats van ze te vragen weer een gebruikersnaam en wachtwoord aan te maken.
- Personaliseer de experience en gebruik uw eigen huisstijl om vertrouwen bij de klant op te bouwen.


VAKTAAL

Progressive profiling houdt in dat u tijdens de customer journey geleidelijk meer gegevens over uw gebruikers verzamelt, in plaats van klanten die uw app voor het eerst gebruiken een ellenlang registratieformulier voor te schotelen. Met een social login kunnen gebruikers toestemming geven om bepaalde algemene gegevens uit hun social media-accounts met u te delen, zodat ze niet alles handmatig hoeven in te vullen en sneller toegang tot uw services krijgen.

Snelle time-to-market

Een moderne Customer Identity-oplossing helpt de time-to-market te verkorten en biedt een breed scala aan tools om identity en access management snel en effectief te integreren in uw klantgerichte apps, websites en portals. Er zijn bijvoorbeeld kant-en-klare oplossingen die snel en eenvoudig kunnen worden geconfigureerd en ingevoerd door organisaties die eenvoudige behoeften hebben op het gebied van identity management en de voorkeur geven aan low-code implementaties. Maar er zijn ook oplossingen met een grote verscheidenheid aan API's (application programming interfaces) en SDK's (software development kits) voor organisaties die meer complexe behoeften hebben en veel aanpassingen moeten uitvoeren. Dankzij deze tools kan een Customer Identity-oplossing snel in uw customer experience worden geïntegreerd en hoeven uw developers niet alles van de grond af op te bouwen. Zo profiteert u van een snellere time-to-market.

Gecentraliseerd beheer

Het centraliseren van identity en access management wordt belangrijker naarmate het aantal customer experiences in uw verschillende kanalen toeneemt. Eén source of truth voor de identities van al uw gebruikers, groepen en devices kan probleemloos met uw organisatie meegroeien, dankzij de lagere administratieve overhead en de centrale interface waarmee u alle verschillende access policies, groepslidmaatschappen en security-policies kunt beheren. Zo zorgt u voor consistentie, dringt u configuratiefouten terug, voorkomt u hiaten in de security en waarborgt u de compliance.

Het beheren van identity en access management voor elke app afzonderlijk is inefficiënt en riskant. Niet alleen is het lastig omdat u veel taken moet herhalen, maar u bent ook kwetsbaar voor gaten in de security omdat u nooit helemaal zeker weet of de access- en security-policies consistent worden toegepast in uw hele digitale omgeving.

Beveiliging op internetschaal

Een moderne Customer Identity-oplossing is gebaseerd op een veilig cloudplatform dat wordt beheerd door de

serviceprovider. U hoeft zich dus geen zorgen te maken over het beveiligen en bijwerken van het onderliggende platform of de infrastructuurcomponenten. Dat valt allemaal onder de verantwoordelijkheid van de serviceprovider.

Daarnaast omvat een moderne Customer Identity-oplossing geavanceerde security-mogelijkheden (zoals adaptive multi-factor authenticatie), biedt ondersteuning voor een hele reeks factoren, houdt rekening met dreigingsinformatie en activeert responses op basis van context. De uitgebreide analyserapporten en dashboards bieden bovendien in real time inzicht in potentiële bedreigingen en aanvallen, zodat teams deze snel kunnen identificeren, onderzoeken en oplossen.

Met een moderne Customer Identity-oplossing kunt u gebruikmaken van de nieuwste innovaties op het gebied van security, zoals op risico gebaseerde policies en passwordless authenticatie, zonder dat u deze zelf hoeft te ontwikkelen. Uw developmentteams kunnen zich richten op de primaire activiteiten van uw organisatie in plaats van zich bezig te houden met de nieuwste security-bedreigingen.

De platformbenadering

Een moderne Customer Identity-oplossing gebruikt een platformbenadering voor identity en access management om elke use case, elke gebruiker en elke technologie te kunnen ondersteunen.

Een platformbenadering biedt uw organisatie de mogelijkheid om identity en access management (IAM)-synergieën te vinden tussen uw verschillende soorten gebruikers (zoals werknemers, partners en klanten) ongeacht hun locatie, app of device. Een B2B-resellerpartner (business-to-business) en een interne sales rep hebben bijvoorbeeld allebei toegang nodig tot dezelfde salestools en -apps, productcatalogussen, enzovoort. Als een organisatie zelf een Customer Identity-oplossing wil ontwikkelen, is de kans groot dat de oplossing door meerdere productteams wordt gebouwd, waarbij het ene team zich bijvoorbeeld richt op de interne use case terwijl het andere team zich focust op de partner use case. Op deze manier creëert elk team een andere user experience en stelt andere security- en access-policies op, waardoor kostbare tijd en resources worden verspild. Het resultaat is bovendien een inconsistente user experience die weer nieuwe security-risico's

kan veroorzaken. Een moderne Customer Identity-oplossing die is gebaseerd op een uniek platform biedt een consistente IAM-benadering voor elke eindgebruiker en maakt optimaal gebruik van synergievoordelen.


TIP

Een onafhankelijke en neutrale platformbenadering breidt bovendien de Customer Identity-mogelijkheden uit omdat uw digitale assets kunnen worden geïntegreerd met elke gewenste technologie. U kunt een soepele connectie tot stand brengen met uw on-prem should this not be: on-premapps? If so it should be on-prem- in Dutch en cloudapps, zodat uw klanten op uniforme wijze toegang kunnen krijgen tot zowel uw legacy als uw moderne producten. En dankzij de pre-built integraties met de allerbeste technologieën kunt u de datapunten uit uw favoriete tools blijven gebruiken. U zou bijvoorbeeld contactgegevens die bij de registratie zijn verzameld kunnen invoeren in een marketingtool die het contact met de klant automatiseert.

Veilige, betrouwbare en schaalbare infrastructuur als basis

Organisaties die een eigen Customer Identity-oplossing bouwen, moeten continu veel tijd en geld besteden aan het ontwerpen, bouwen en onderhouden van de infrastructuur die de basis vormt voor de security, betrouwbaarheid en schaalbaarheid waar een succesvolle organisatie van afhankelijk is.

Is de security niet op orde, dan verliezen uw klanten het vertrouwen in uw merk en gaan ze naar de concurrent. Laat de betrouwbaarheid te wensen over, dan is uw site regelmatig onbereikbaar en hebben uw gebruikers geen toegang tot uw services. En is de schaalbaarheid onvoldoende, dan duurt het inloggen tijdens een verkeerspiek veel te lang en gaan uw klanten liever ergens anders naartoe.


HERINNERING

Een moderne Customer Identity-oplossing is gebaseerd op een veilige, betrouwbare en schaalbare cloud-native infrastructuur en wordt geleverd als een service.

Dat betekent dat u zich geen zorgen hoeft te maken over het inhuren van dure infrastructuurexperts, de verbruikskosten van

de cloudinfrastructuur of het opschalen van de infrastructuur om pieken in de vraag op te vangen. Ook hoeft u zich niet bezig te houden met patches, upgrades en onderhoud van software en systemen die veel tijd in beslag nemen en waarvoor de service aan de klant moet worden onderbroken.

Voor een goede betrouwbaarheid moet een moderne Customer Identity-oplossing een zeer hoge redundantie bieden op elke laag van de infrastructuur-stack voor het geval een server- of netwerkverbinding uitvalt. Deze redundante infrastructuur moet zijn voorzien van geautomatiseerde workflows die het verkeer zo nodig kunnen omleiden naar verschillende geografische locaties om een maximale uptime te bieden zonder dat menselijke tussenkomst nodig is.

ARDUINO

Arduino streeft ernaar de Internet of Things (IoT)-revolutie democratischer te maken door opensourcesoftware en -hardware toegankelijk te maken voor leerkrachten, studenten en allerlei soorten makers. Omdat Arduino in Europa gevestigd is, moet de organisatie voldoen aan de zeer strenge privacy- en securitybepalingen van de Algemene verordening gegevensbescherming.

Via het platform van Auth0 kon Arduino snel tweefactorauthenticatie implementeren en zo voldoen alle wettelijke voorschriften en de hoogste securitynormen toepassen. Ook kon de back-end van Arduino sneller worden opgeschaald en konden developers producten sneller lanceren.

Voor Arduino IoT Cloud, de app van Arduino, hadden developers zowel IoT- als Android-logins nodig. Dat was in tweeënhalve dag geregeld, zodat het product een aantal weken eerder dan gepland kon worden uitgerold.

SIEMENS

Bij Siemens vinden in diverse bedrijfsonderdelen allerlei verschillende processen plaats. Het was daarom dringend nodig om de inlogprocessen van de organisatie te standaardiseren en te beveiligen. Twee jaar geleden nam Siemens Auth0 in de arm om een uniform inlogproces voor zijn klanten en partners te creëren.

Samen ontwikkelden ze Siemens ID, een gecentraliseerde inlogservice die snel kan worden geïntegreerd in de applicatie-stack van alle bedrijfsonderdelen. Alle klanten en partners over de hele wereld gebruiken Siemens ID om toegang te krijgen tot de honderden apps en services van Siemens. Met Siemens ID is het mogelijk de gebruikersdatabase en de inlogpagina gecentraliseerd op te slaan en kunnen individuele bedrijfsonderdelen de applicatie op hun eigen specifieke manier integreren.

Voor een goede schaalbaarheid heeft u on-demand capaciteit nodig die automatisch kan op- of afschalen. Op deze manier verspilt u geen geld aan ongebruikte capaciteit en loopt u geen omzet mis als gevolg van onvoldoende capaciteit.

Tot slot moet u voor een goede security voortdurend op de hoogte zijn van de nieuwste bedreigingen en kwetsbaarheden voor uw hele infrastructuur-stack.


TIP

Een externe Customer Identity-partner kan al deze vereisten voor uw organisatie beheren, zodat u zich op uw kernactiviteiten kunt richten.

Verschillende use cases

Een moderne Customer Identity-oplossing helpt organisaties een breed scala aan use cases te ondersteunen om aan verschillende zakelijke behoeften te voldoen. In de volgende gedeelten gaan we dieper in op enkele veelvoorkomende use cases en bespreken we een paar ervaringen van Okta-klanten.

Bescherming tegen account takeovers

Een account takeover is een identity attack-methode die steeds vaker voorkomt. Hierbij verschaft een aanvaller zich op onbevoegde wijze toegang tot het account van een gebruiker om daar financieel voordeel uit te halen of om data te stelen. Deze aanvallen kunnen handmatig, maar ook automatisch door bots worden uitgevoerd. U kunt account takeovers voorkomen met een identity-platform dat security combineert met een frictieloze user experience.

Uiterst schaalbare applicaties

Organisaties bouwen apps en websites om zoveel mogelijk klanten aan te trekken. Dat betekent dat uw Customer Identity-oplossing betrouwbaar en schaalbaar moet zijn, vooral wanneer er een piek in het verkeer of in de vraag van de klant is. Bijvoorbeeld als er tickets voor een concert of een sportwedstrijd worden verkocht of tijdens een flitsverkoop in de vakantie.

Samenvoeging van customer identities uit verschillende applicaties

Uw klanten vinden het vervelend om zich te registreren voor nieuwe accounts en om meerdere inloggegevens te beheren voor verschillende apps en websites, vooral als deze bij dezelfde organisatie of hetzelfde merk horen. Het samenvoegen van customer identities voor al uw digitale assets is daarom cruciaal voor het creëren van een frictieloze customer experience.

Integratie van enterprise-identities

Met een moderne Customer Identity-oplossing hoeven B2B-klanten geen verschillende identities en inloggegevens meer aan te maken wanneer ze de apps, websites en portals van partners willen gebruiken. In plaats daarvan worden hun enterprise-identities door de Customer Identity-oplossing geïntegreerd, zodat B2B-klanten hun bestaande zakelijke identities en inloggegevens ook in de digitale omgeving van hun partners kunnen gebruiken.

BAZAARVOICE

Na een aantal jaren van snelle groei constateerde Bazaarvoice dat zijn productaanbod voor klanten slecht geïntegreerd was. IT kreeg de taak om de user identities voor alle producten te consolideren.

Bazaarvoice is klant-gebruikers nu aan het onboarden voor de inmiddels gekoppelde apps en overweegt gebruik te maken van de inbound federation-opties van Okta, waarmee klanten zouden kunnen inloggen via hun eigen identity provider. Deze federation zou het user management voor klanten vereenvoudigen en de gebruikersauthenticatie en gegevensopslag voor de meer dan 590 miljoen klanten die de app van de organisatie elke maand gebruiken, voor Bazaarvoice in goede banen leiden.

XERO

Xero bereidde zich voor op een periode van sterke groei en de IT-afdeling was op zoek naar een identity management-partner die de applicatie-infrastructuur kon beveiligen en processen kon automatiseren. Okta Workflows bleek de perfecte oplossing te zijn.

In scripts voor geautomatiseerde processen met aangepaste code moeten vaak sleutels, tokens of wachtwoorden worden geïntegreerd waarmee API's van derden kunnen worden aangeroepen. Zulke tokens worden gewoonlijk opgeslagen in een bestand op de server van de organisatie, die niet altijd even goed beveiligd is. Omdat Workflows op het Okta-platform draait en niet op een on-prem computer of server, worden API-tokens automatisch beveiligd en bijgewerkt.

Veilige toegang tot API's

Voor organisaties die willen deelnemen aan de API-economie (besproken in hoofdstuk 2), is de bescherming van de toegang tot API's van cruciaal belang om te voorkomen dat kwaadwillenden

misbruik van kwetsbaarheden maken of onbevoegde toegang tot gekoppelde applicaties krijgen.

IN DIT HOOFDSTUK

- **Belangrijkste mogelijkheden van een Customer Identity-oplossing**
- **Ondersteuning voor alle use cases met een onafhankelijk en neutraal platform**
- **Betrouwbare en veilige service op grote schaal**
- **Samenwerking met een marktleider**

Hoofdstuk 5

Waar u op moet letten bij een moderne Customer Identity-oplossing

Als u weet hoe u met een moderne Customer Identity-oplossing een veilige en frictieloze customer experience (CX) kunt creëren (zie hoofdstuk 4), kunt u beginnen met het verkennen van uw opties. In dit hoofdstuk gaan we dieper in op de mogelijkheden en functies die een moderne Customer Identity-oplossing moet bieden.

Het beste product vinden

Een moderne Customer Identity-oplossing moet standaard mogelijkheden bieden die u eenvoudig en snel kunt configureren en implementeren, alsmede developervriendelijke tools, zoals API's (application programming interfaces), SDK's (software development kits) en hooks, om de Customer Identity-oplossing verder te personaliseren en uit te breiden.

Hier volgen enkele standaard mogelijkheden die CIAM moet bieden:

- **Authenticatie, autorisatie en user management** zijn de belangrijkste vereisten voor elke Customer Identity-oplossing (zie hoofdstuk 1). Deze drie basismogelijkheden zouden daarnaast de volgende geavanceerde functies moeten bieden:
  - *Authenticatie:* ondersteuning voor social logins en generieke OIDC (OpenID Connect); single sign-on voor applicaties van derden; passwordless authenticatie; op risico gebaseerde authenticatie; een pre-built aanmeldwidget; gepersonaliseerde branding op applicatieniveau.
  - *Autorisatie:* API access management op basis van OAuth 2.0 (open autorisatie); integratie met API-gateways; op rollen gebaseerde toegangscontrole voor applicaties.
  - *User management:* een zeer schaalbare user store in de , cloud om al uw gebruikers, groepen en devices te beheren; toewijzing van gebruikersprofielen; ondersteuning voor de wijze waarop u gebruikers wilt migreren (bulkimport, just-in-time, bestaande directory).
- **Vooraf gedefinieerde en personaliseerbare gebruikersflows** die snel eersteklas supportfuncties voor gebruikers en klanten kunnen leveren, zoals selfservice voor het registreren, het resetten van wachtwoorden en het herstellen van accounts en/of gebruikersnamen.
- **Gecentraliseerd beheer inclusief een intuïtieve interface** en personaliseerbare dashboards die security- en admin-teams kunnen gebruiken om security-policies centraal en consistent te beheren.
- **MFA (multi-factor authenticatie) en adaptive MFA** met ondersteuning voor verschillende factoren en methoden, van eenvoudige e-mails en sms'jes tot meer geavanceerde methoden, zoals biometrie (bijvoorbeeld TouchID en FaceID). Adaptive MFA voegt een op risico gebaseerde, intelligente authenticatielaag toe om op basis van contextafhankelijke informatie (zoals locatie en device) alleen MFA af te dwingen wanneer het nodig is.
- **Geautomatiseerde provisioning met lifecycle management** waaronder geautomatiseerde workflows die zijn gekoppeld aan de lifecycle-fase van de klant, zodat u gebruikers kunt provisioneren en deprovisioneren voor

downstream-apps en -systemen in uw hele technologiestack. U zou bijvoorbeeld B2B-partners direct bij de start van de partnerrelatie automatisch toegang tot CRM kunnen verlenen.

- **B2B-integratie (business-to-business) om een connectie** met apps en portals van partners tot stand te brengen en identities te samenvoegen of bundelen voor verschillende enterprise directory's, zoals Active Directory en LDAP (Lightweight Directory Access Protocol). Op deze manier kunnen zakelijke gebruikers eenvoudiger inloggen (zonder nieuwe inloggegevens aan te maken) en beschikken organisaties die Customer Identity gebruiken altijd over de meest recente gegevens van hun zakelijke gebruikers.
- **Integratie met legacy on-prem apps** om uw klanten op uniforme wijze toegang tot al uw producten te bieden en uw digitale transformatie te versnellen.

Organisaties die niet genoeg hebben aan deze standaard mogelijkheden, kunnen een oplossing kiezen die een breed scala aan API's, SDK's en hooks biedt voor de programmeertalen die uw developmentteams gebruiken. Deze developervriendelijke tools komen goed van pas bij de volgende taken:

- **Snel en efficiënt Customer Identity in uw apps integreren** zonder dat u een build op maat van de grond af moet opbouwen.
- **Customer Identity personaliseren en branding toevoegen** om CX op maat te bieden en een concurrentievoordeel te behalen.
- **De beste oplossingen van uw tech stack benutten om uw Customer Identity**-mogelijkheden uit te breiden en uw klanten nog meer opties te bieden (zie het volgende gedeelte voor meer bijzonderheden).

Het juiste platform kiezen

Zoek een Customer Identity-oplossing die is gebouwd op een open, onafhankelijk en neutraal platform. U heeft dan een veilige basis voor elke identity use case, voor elke eindgebruiker die communiceert met uw organisatie en voor elke technologie die u wilt gebruiken.

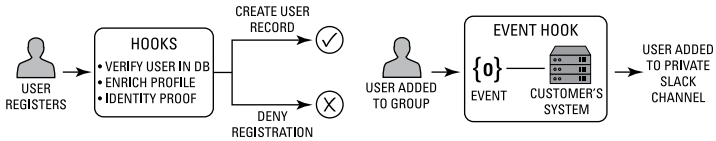
Kies een Customer Identity-oplossing die zoveel mogelijk typen eindgebruikers ondersteunt, zoals consumenten, partners en zelfs uw werknemers. Met een platformbenadering bent u goed voorbereid op de toekomst. En dat is belangrijk omdat de kans groot is dat uw behoeften na verloop van tijd veranderen. Uw organisatie is bijvoorbeeld nu op zoek naar een Customer Identity-oplossing die standaard B2B-integratie voor een partnerportal biedt. Maar over een jaar wil uw organisatie misschien ook consumenten als eindgebruikers toevoegen en heeft u personaliseerbare, passwordless authenticatie nodig voor een nieuwe mobiele B2C-app (business-to-consumer). Als u voor een platformbenadering heeft gekozen, heeft u hiervoor geen twee afzonderlijke Customer Identity-oplossingen nodig. U kunt beide use cases beheren met één platformgebaseerde Customer Identity-oplossing die dankzij het eenvoudige beheer en de vereenvoudigde workflows ook nog eens verschillende kostenbesparingen en efficiëntieverbeteringen oplevert. En misschien wil uw organisatie na verloop van tijd ook de identity en access management-mogelijkheden voor uw werknemers stroomlijnen. Al deze typen gebruikers kunnen naadloos worden beheerd via hetzelfde Customer Identity-platform.

Met een platformbenadering kunt u bovendien superieure oplossingen kiezen voor al uw use cases en alle specifieke componenten van uw tech stack, zowel on-prem als in de cloud. Zo kunt u altijd de beste tool gebruiken die beschikbaar is in plaats van genoegen te nemen met middelmatige oplossingen die in een bundel zijn samengevoegd. Ga dus op zoek naar een Customer Identity-oplossing die een groot aantal pre-built integraties met de belangrijkste applicaties en services in uw tech stack biedt, zoals:

- API-gateways
- Bot-detectie
- Integrators voor klantdata
- Identity proofing
- Infrastructure-as-a-service
- Vertrouwelijk access management
- Security-analytics

Het is ook belangrijk dat een oplossing no-code connectors biedt, zodat uw teams geautomatiseerde workflows voor uw belangrijkste technologieën kunnen bouwen zonder zelf code te hoeven schrijven.

Tot slot moet uw Customer Identity-oplossing eenvoudige integratie via API's, SDK's en hooks bieden. Inline hooks bieden developers de mogelijkheid om Customer Identity-processen aan te passen met eigen logica en data uit een externe bron. En met event hooks kunnen Customer Identity-events via een HTTP Post naar een downstream-systeem worden gestuurd op het moment dat ze zich voordoen (net als bij een webhook). Afbeelding 5- 1 toont een voorbeeld van een inline hook en een event hook.



AFBEELDING 5-1: een voorbeeld van een inline hook (links) en een event hook (rechts).

Vertrouwde infrastructuur beveiligen

Een belangrijk voordeel van een moderne Customer Identity-oplossing is dat deze wordt geleverd als een service. U hoeft dus geen infrastructuur aan te schaffen en te onderhouden om de schaalbaarheid, betrouwbaarheid en security te bieden die organisaties nodig hebben in de dynamische en snel veranderende digitale economie. Het is met name belangrijk dat een moderne Customer Identity-oplossing de volgende mogelijkheden biedt:

- **Schaalbaarheid:** uw oplossing moet het schaalniveau ondersteunen dat uw organisatie nu en in de toekomst nodig heeft. U wilt niet dat het systeem uitvalt of een bottleneck voor het verkeer vormt wanneer uw apps viraal gaan en de vraag explosief stijgt. En het is ook niet handig als u uw Customer Identity-leverancier moet vervangen omdat deze de groei van uw organisatie niet kan bijhouden. Zoek een Customer Identity-oplossing die kan opschalen naar honderdduizenden authenticaties per minuut en een leverancier waarvan bekend is dat deze blijft investeren in vernieuwingen van de oplossing.

- **Betrouwbaarheid:** zoek een Customer Identity-partner die de hoogste uptime garandeert en deze ook daadwerkelijk levert. Downtime leidt tot misgelopen omzet, reputatieschade en mogelijk verlies van klanten die vanwege de slechte customer experience en slechte reviews overstappen naar de concurrent. Ook al heeft u de beste producten van allemaal, als uw klanten er geen toegang toe hebben speelt dat geen enkele rol.
- **Security:** kies een Customer Identity-partner die u beschermt tegen credential stuffing-aanvallen, waarbij misbruik wordt gemaakt van gecompromitteerde en gelekte inloggegevens. Bij aanvallen met inloggegevens worden zwakke, veelgebruikte of gestolen identity-gegevens gebruikt om legitieme gebruikers na te bootsen of legitieme accounts over te nemen. Zo wordt bij credential stuffing-aanvallen bijvoorbeeld gebruikgemaakt van gebruikersnamen en wachtwoorden die zijn gestolen tijdens datalekken, verkregen door middel van phishing-campagnes of gekocht op onlineforums. Aanvallers gebruiken vervolgens geautomatiseerde tools om deze inloggegevens te testen bij andere online services. Bij brute force- en password spray-aanvallen worden zwakke, veelgebruikte wachtwoorden systematisch en automatisch getest, vaak in combinatie met een reeks bekende gebruikersnamen.

Uw Customer Identity-oplossing heeft rechtstreeks invloed op uw CX en uw organisatie. Uw klanten zullen uw Customer Identity-provider niet de schuld geven als er problemen optreden met schaalbaarheid, betrouwbaarheid en security. Ze zien het als uw verantwoordelijkheid en stappen over naar de concurrent als u niet aan hun verwachtingen voldoet. U kunt dus het beste samenwerken met een vertrouwde partner die een goede reputatie heeft en een moderne Customer Identity-oplossing levert die buitengewoon goed presteert op het gebied van schaalbaarheid, betrouwbaarheid en security.

Een marktleider kiezen

Tot slot moet u bij het evalueren van de verschillende Customer Identity-oplossingen ook de partner aan een grondig onderzoek onderwerpen. Customer Identity is een journey die altijd doorgaat

en dat betekent dat u een partner nodig heeft die uw succes op de lange termijn op het oog heeft. Ga dus niet in zee met een 'eenmalige' leverancier die u zijn product verkoopt en verder niet naar u omkijkt. De verwachtingen van klanten blijven zich ontwikkelen, net als de security-bedreigingen, wettelijke verplichtingen en technologische innovaties. Overweeg een partner die marktleider is op dit gebied en die u bijvoorbeeld kunt herkennen aan de volgende criteria:

- **Validaties van onafhankelijke derden,** waaronder analistenrapporten en certificeringen, zoals:
  - SOC 2-rapport (Service Organization Control) type I en type II
  - STAR-certificering (Security, Trust & Assurance Registry) van de CSA (Cloud Security Alliance) niveau 2
  - ISO 27001:2013- en ISO 27018:2014-certificering (International Organization for Standardization
- **Naleving van wettelijke verplichtingen,** zoals de AVG (Algemene verordening gegevensbescherming) en de HIPAA (Health Insurance Portability and Accountability Act).
- **Expertise die blijkt uit referenties en verhalen van klanten die relevant zijn voor uw sector,** grootte en geografische locatie en waarmee u rechtstreeks contact kunt opnemen.
- **Een toekomstbestendige oplossing,** zoals blijkt uit de voortdurende innovaties, de product-roadmaps, het thought leadership en de deelname aan developer-community's en standaardisatiegroepen.

IN DIT HOOFDSTUK

- **Het pad naar Customer Identity-maturiteit**
- **Het eerste begin**
- **Automatische groei en opschaling**
- **Optimalisatie van de customer experience en handhaving van security**
- **De marktleider zet de nieuwe standaard**

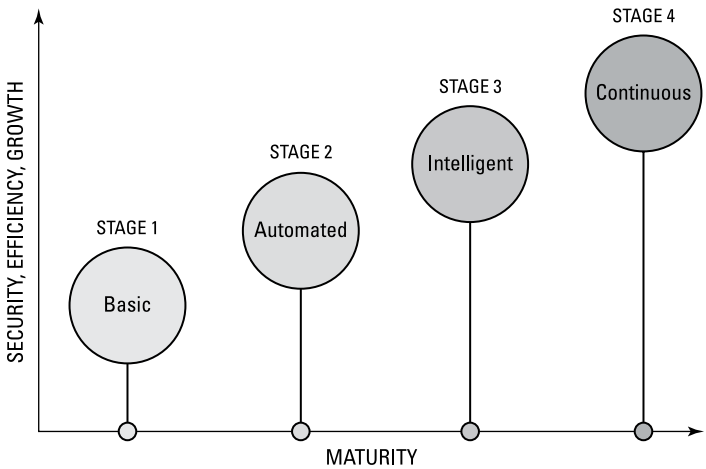
Hoofdstuk **6**

Het potentieel van Customer Identity benutten voor de behoeften van uw organisatie

In hoofdstuk 5 hebben we uitgelegd waar u op moet letten bij een moderne Customer Identity-oplossing, maar waar moet u beginnen? Uw organisatie is uniek en u wilt er zeker van zijn dat de oplossing die u kiest zo goed mogelijk bij uw specifieke behoeften past. In dit hoofdstuk gaan we dieper in op waar en hoe u de eerste stappen zet op uw pad naar customer identity and access management-maturiteit.

Het pad naar Customer Identity-maturiteit

In welke fase uw organisatie zich ook bevindt op het pad naar Customer Identity-maturiteit, elke fase levert uitdagingen op waar alle organisaties mee te maken krijgen. Aan de hand daarvan kunnen we dit pad in vier fasen onderverdelen: Basis, Automatisering, Intelligentie en Continuïteit (zie afbeelding 6- 1).



AFBEELDING 6-1: Waar staat uw organisatie op de Customer Identity-maturiteitscurve?

In elke fase kunt u een aantal duidelijke stappen zetten op weg naar continuïteit op het gebied van customer identity and access management. In de volgende gedeelten nemen we de verschillende fasen onder de loep, zodat u kunt zien wat dit betekent voor uw organisatie.

Basis: bouwen of kopen

Dit is de eerste fase. Vanuit zakelijk oogpunt gezien bent u net begonnen en wilt u proberen of uw product een goede positie op de markt kan veroveren. Uw organisatie heeft bijvoorbeeld een

geweldig idee voor een nieuwe klanten-app en u wilt deze zo snel mogelijk van de grond krijgen. Uw app zit aan het begin van de development-lifecycle en u wilt de levensvatbaarheid bepalen. De focus van uw team ligt op het ontwikkelen, bouwen en valideren van de business case van de app, maar het team is maar klein. U moet dus keuzes maken.

Uw doelstellingen aan de ene kant:

- U wilt een minimaal levensvatbaar product zo snel mogelijk op de markt brengen en heeft daarvoor eenvoudig identity management nodig.
- U wilt uw product aan potentiële klanten aanbieden.
- U wilt aantonen dat u het juiste probleem voor uw klanten oplost.

De uitdagingen die u het hoofd moet bieden aan de andere kant:

- U wilt uw product op de markt brengen en iteraties uitvoeren op basis van de informatie die u verzamelt
- U loopt het risico dat algemene security-problemen het hele project onderuit halen
- U heeft beperkte engineering resources en weet niet precies waar identity management in het ontwerp past

Dit is de eerste fase van het pad naar Customer Identity-maturiteit. In de fase Basis moet u beslissen of u uw beperkte tijd en kostbare resources wilt besteden aan het bouwen van uw eigen Customer Identity-oplossing of dat u beter met een externe provider in zee kunt gaan.

Zoals in hoofdstuk 3 is uitgelegd, neemt het intern bouwen en beheren van tools kostbare tijd van uw developers en engineers in beslag. Deze tijd zouden ze beter kunnen besteden aan de producten die belangrijk zijn voor de kernactiviteiten van uw organisatie. Daarom kunt u beter een externe oplossing gebruiken om snel de belangrijkste Customer Identity-mogelijkheden te implementeren die u nodig heeft (authenticatie, autorisatie en user management). Hiermee legt u een goede basis voor het leveren van veilige access experiences aan uw klanten terwijl u tegelijkertijd de efficiëntie van uw developers maximaliseert.

Volgens een Harris Poll-onderzoek dat werd uitgevoerd door Stripe.com besteden developers gemiddeld 17,3 uur per week aan het opsporen van fouten en het onderhouden van legacy en slechte code. Een moderne Customer Identity-oplossing kan de development versnellen en u veel onderhoudstaken uit handen nemen, zodat u zich kunt richten op de kernactiviteiten van uw organisatie.

Als uw organisatie de fase Basis op de Customer Identity-maturiteitscurve heeft afgerond, heeft u cruciale functies voor Identity-security in uw app geïntegreerd en de app met succes op de markt gebracht. Vervolgens kunt u nadenken over het uitbreiden van uw product om een groeiend klantenbestand te bedienen.

Automatisering: centraliseren en opschalen

Gefeliciteerd! Uw applicatie was een groot succes en u wilt nu aanvullende producten voor uw klanten ontwikkelen. U neemt mensen aan en u heeft al een CTO, een VP of Product of een VP of Engineering gevonden die leiding aan het project geeft. Maar deze nieuwe groeifase brengt ook een reeks nieuwe uitdagingen met zich mee. Het groeiende aantal betalende klanten vraagt bijvoorbeeld om meer geavanceerde functies of functies van enterpriseniveau waaraan u mogelijk geen gehoor kunt geven omdat u onvoldoende tijd of ervaring heeft. U moet dus prioriteiten stellen aan uw initiatieven om effectief op te schalen en te blijven groeien.

Vanuit Customer Identity-standpunt gezien zou u kunnen overwegen zelf identity-mogelijkheden te bouwen omdat deze zo belangrijk zijn voor uw klanten. Maar u kunt u beter richten op andere belangrijke doelen, zoals het bouwen en lanceren van nieuwe producten om uw klantenbestand verder uit te breiden.

U zit nu in de fase Automatisering waarin de juiste externe Customer Identity-oplossing u kan helpen op deze gebieden:

- Het management (en de bijbehorende risico's) van externe customer identities uitbesteden. Uw eindgebruikers moeten kunnen inloggen via bestaande identity providers en u moet

de authenticatie kunnen delegeren aan een bestaande Active Directory of LDAP-directory (Lightweight Directory Access Protocol). Op deze manier kan uw organisatie het user management centraliseren en moeiteloos opschalen.

- Moderne authenticatiestandaarden gebruiken, zoals OpenID Connect, OAuth en SAML (Security Assertion Markup Language) om automatisch de nieuwste security- en identity-practices te adopteren zonder dat u voortdurend achter de feiten aanholt.
- Verschillende compliancevereisten naleven, zoals de AVG (Algemene verordening gegevensbescherming) en de CCPA (California Consumer Privacy Act).
- Processen zoals provisioning en deprovisioning automatiseren met customer lifecycle management.
- De security aanscherpen wanneer uw organisatie opschaalt en een aantrekkelijker doelwit voor aanvallers vormt. Dit kan bijvoorbeeld door automatisch onveilige of uitgelekte wachtwoorden te detecteren.
- Uw klanten moderne manieren bieden om hun wachtwoord te resetten of zich te authenticeren (via sms, spraakoproep, e-mail of eenmalige wachtwoorden) en deze security-policies beheren in een gecentraliseerde admin console.

Als u de fase Automatisering op de Customer Identity-maturiteitscurve heeft doorlopen, heeft u het bereik van uw product uitgebreid en biedt u meer geavanceerde mogelijkheden voor user management, compliance en security. Als u wilt blijven opschalen, moet u investeren in krachtigere security en nieuwe functies voor de customer experience.

Intelligentie: compromisloos optimaliseren

In deze fase bevinden organisaties zich in een goede positie om marktleider te worden. Als ze willen blijven groeien, moeten ze hun product optimaliseren en tegelijk rekening houden met de identity-vereisten van de verschillende interne belanghebbenden (zoals de product-, engineering- en marketingteams) die er allemaal naar streven om een grootschalige, frictieloze en customer experience te bieden.

Een moderne Customer Identity-oplossing helpt u de tegenstrijdige belangen van deze belanghebbenden met elkaar in evenwicht te brengen en uw infrastructuur te verbeteren met behulp van API's (application programming interfaces) en microservices die allerlei taken kunnen overnemen, zoals:

- Geavanceerde onboarding-experiences met een hoger zekerheidsniveau bieden met behulp van identity proofing en accountverificatie.
- Een frictieloze customer experience bieden met robuuste security die is gebaseerd op oplossingen zoals adaptive multi-factor authenticatie (een adaptieve intelligentie-laag die aan de hand van contextafhankelijke informatie en gedragspatronen het risico vaststelt en eventueel om aanvullende authenticatie vraagt), passwordless authenticatie (bijvoorbeeld via WebAuthn of e-mails met magic links) en progressive profiling waarmee geleidelijk steeds meer kenmerken van gebruikers in profielen worden vastgelegd.
- De nieuwste vereisten op het gebied van privacy- en security-compliance naleven door de user lifecycle en het data management te consolideren in een centraal systeem.
- Alles optimaliseren door de Customer Identity-mogelijkheden uit te breiden naar uw volledige tech stack met behulp van pre-built integraties of workflows op maat, en door gebruik te maken van de allerbeste technologieën (bijvoorbeeld tools voor het blokkeren van bots, het beheren van klantrelaties en het uitvoeren van marketinganalyses).

Op dit punt biedt de applicatie uw klanten een krachtige, mogelijk zelfs passwordless bescherming. Uw gebruik en opslag van klantdata bieden mogelijkheden voor betere personalisering en is volledig conform de wetgeving op het gebied van dataprivacy. Dankzij de toonaangevende integraties wordt de identity-security zeer strikt uitgevoerd en kunt u proactief risico's detecteren en terugdringen. Klanten vinden uw services betrouwbaar en gebruiksvriendelijk en u bevindt zich in een uitstekende positie om andere geavanceerde functionaliteiten te verkennen.

Continuïteit: als marktleider de nieuwe standaard zetten

Deze laatste fase van de Customer Identity-maturiteitscurve wordt bereikt door marktleiders die de digitale transformatie hebben doorlopen. Deze organisaties hebben een speciaal intern Customer Identity-team dat zich richt op het ondersteunen van een omnichannel-strategie die zowel de security als de customer experience optimaliseert. Als marktleider onderscheiden ze zich van de concurrentie omdat ze een goed inzicht in identity management hebben. Ze beseffen dat identity management zich blijft ontwikkelen en een strategie op de lange termijn nodig heeft.

Organisaties die aan de top willen blijven staan moeten voortdurend de standaard voor uitmuntendheid zetten. In deze fase omvat Customer Identity veel meer dan een frictieloze en veilige inlog-experience voor uw klanten. Customer Identity moet ook helpen bij het uitvoeren van de volgende taken:

- Uw klanten volgen in alle kanalen (webstores, mobiele stores en fysieke winkels) om een 360-graden klantbeeld op te bouwen, zodat u in elk kanaal gepersonaliseerde experiences kunt bieden.
- Fijnmazige autorisatie en op risico gebaseerde autorisatie implementeren om de toegangscontrole te maximaliseren op elk moment dat data kan worden onderschept, alsmede aan zeer strenge industriestandaarden voldoen, zoals FAPI (Financial-grade API), en de frictie voor klanten tot een minimum beperken. U kunt risicosignalen instellen voor categorieën zoals netwerk, locatie, device en type transactie. Ook kan er dynamisch een risicoscore worden berekend of geactiveerd op basis van bepaalde voorwaarden (zoals tijdstippen en user events).
- De security-orkestratie en -respons automatiseren met flexibele workflows, alsmede de hoeveelheid tijd en moeite terugdringen die aan het beheren van identity- en security-policies wordt besteed door gebruik te maken van artificial intelligence en machine learning.

Of u nu een beginnende productdeveloper of een gevestigde marktleider bent, het integreren van Customer Identity in uw product-roadmap is van cruciaal belang. Als u weet in welke fase van de Customer Identity-maturiteitscurve uw organisatie zich bevindt, kunt u de prestaties monitoren en u op bepaalde onderdelen richten die een concurrentievoordeel opleveren.

IN DIT HOOFDSTUK

- **Aantrekkelijkere customer experiences bieden**
- **Vertrouwen scheppen en betere securityresultaten behalen met uw merk**
- **Regelnaleving en privacybescherming van gebruikers**
- **Ondersteuning voor steeds complexere architecturen en use cases**

Hoofdstuk 7

Hoe zal de toekomst van Customer Identity eruitzien?

In dit hoofdstuk kijken we vooruit en nemen we vier belangrijke trends onder de loep die de toekomst van Customer Identity vormgeven en leggen we uit hoe uw organisatie hiervan de vruchten kan plukken.

De klantenbinding verbeteren

Klantgerichte organisaties moeten de manier waarop gebruikers in contact komen met hun merk voortdurend vernieuwen en verbeteren om de klantenbinding te verhogen en de lifetime value van klanten te maximaliseren. Het is dus logisch dat een betere klantenbinding en een snellere time to value tot de belangrijkste trends behoren die de toekomst van Customer Identity gaan bepalen. Als u een nieuw product ontwikkelt, wilt u dat gebruikers zich betrokken voelen bij dat product. Het bieden

van een superieure customer experience (CX) is van vitaal belang voor het opbouwen van sterke klantrelaties.


TIP

Een moderne Customer Identity-oplossing die is gebouwd met het oog op de toekomst kan de klantenbinding van uw organisatie als volgt verbeteren:

- **Tijdens de customer journey op het juiste moment de juiste persoon om de juiste hoeveelheid informatie vragen.** In plaats van zoveel mogelijk informatie over potentiële nieuwe klanten te verzamelen via een ellenlang registratieproces, kunt u innovaties zoals progressive profiling gebruiken om de frictie voor klanten tot een minimum te beperken en het conversiepercentage te verbeteren.
- **Klanten de juiste content bieden in de taal en de vorm die hen het meest aanspreekt.** Bouw vertrouwen op door uw klanten in hun eigen taal aan te spreken en beheer de vertaling en de personalisatie afzonderlijk.
- **Uw merk weergeven bij elk contactmoment met de klant om vertrouwen op te bouwen en de relatie te versterken.** Integreer uw merkmateriaal bij elke stap in de customer identity journey. U kunt bijvoorbeeld een SDK (software development kit) of een API (application programming interface) gebruiken om een MFA-app (multi-factor authenticatie) in uw eigen huisstijl voor uw klanten te maken.


HERINNERING

Het creëren van een prettige CX is een van de snelste manieren om de klantenbinding te bevorderen. Klanten die zich betrokken voelen komen vaker terug en kopen meestal meer producten.

Security-resultaten verbeteren

Een moderne Customer Identity-oplossing moet het juiste evenwicht bieden tussen security en CX om bij te dragen aan een vertrouwde relatie tussen uw klanten en uw merk. De security-bedreigingen veranderen voortdurend en worden steeds geraffineerder en gevaarlijker. Het kan dan ook zeer verleidelijk zijn om de security te maximaliseren ten koste van het gebruiksgemak.

In plaats daarvan kunnen organisaties zich beter richten op het optimaliseren van de security-resultaten (voor zichzelf en voor hun klanten). Dit kan bijvoorbeeld door gebruikers zelf het gewenste niveau van data security te laten bepalen, en door security-controles toe te voegen waarvoor geen rechtstreekse invoer van de klant nodig is. Het einddoel moet niet meer security, maar betere security zijn.


TIP

Organisaties kunnen beter niet de meest strikte en ontwrichtende security-opties implementeren die een moderne Customer Identity-oplossing biedt. Het is veel beter om te focussen op het toepassen van de juiste security op het juiste moment en op het opstellen van flexibele policies die de customer experience zo eenvoudig mogelijk houden.

Gebruik de volgende tips om betere security-resultaten te boeken en het opbouwen van vertrouwen in uw merk te vereenvoudigen:

- **Pas op het juiste moment in de customer journey het juiste niveau van security toe.** Zelfs organisaties die duizenden klantgerichte apps hebben, kunnen alles nog steeds eenvoudig laten verlopen door op het juiste moment in de customer journey (zoals tijdens de registratie) alleen de minimale hoeveelheid gegevens op te vragen, zodat de klant zo weinig mogelijk frictie ervaart. Vraag uw klanten bijvoorbeeld alleen om MFA wanneer het nodig is, bijvoorbeeld wanneer ze inloggen vanaf een verdachte locatie of vanaf een onbekend device.
- **Gebruik voor elke applicatie een andere security-policy om het optimale evenwicht te bereiken tussen frictie voor de klant en het risico voor de security.** Apps waarmee klanten zich registreren en aankopen doen hebben bijvoorbeeld een hoger security-niveau nodig dan apps waarmee klanten alleen de status van een bestelling kunnen checken, ook als het om dezelfde gebruiker en hetzelfde merk gaat.
- **Bied eindgebruikers de mogelijkheid om zich aan te melden voor MFA.** In plaats van uw klanten te verplichten zich te registreren voor MFA, kunt u ze ook zelf laten kiezen of ze hier gebruik van willen maken. Hoewel MFA steeds meer wordt gebruikt, vinden veel mensen het nog steeds irritant. U zou in plaats van MFA ook andere risicofactoren kunnen gebruiken waarvoor de klant niets hoeft in te voeren (bijvoorbeeld informatie over device, locatie of netwerk).

- **Bied uw klanten de mogelijkheid om hun account te herstellen via elke factor.** Het is altijd een goed idee om klanten flexibele selfservice-opties te bieden (bijvoorbeeld via e-mail, sms en eenmalige wachtwoorden) waarmee ze hun account kunnen herstellen of hun wachtwoord kunnen resetten zonder tussenkomst van het callcenter.
- **Breid Customer Identity uit naar elk contactmoment zodat u services van derden kunt integreren.** Maak gebruik van speciale technologieën om functionaliteit toe te voegen en de CX te verbeteren op elk contactmoment in de customer journey.

Privacy beschermen

Privacywetten, zoals de AVG (Algemene verordening gegevensbescherming) en de CCPA (California Consumer Privacy Act), hebben nu al veel invloed op de wijze waarop zaken worden gedaan. En er komen wereldwijd steeds meer regels en wetten bij om klanten meer controle over hun persoonsgegevens te geven. Organisaties die het vertrouwen van klanten willen behouden, moeten hier dus op inspelen. Privacy is echter een complex begrip en houdt meer in dan alleen de 'toestemming' van de klant. Vanuit een Customer Identity-standpunt gezien moeten toekomstige mogelijkheden op drie primaire use cases zijn gericht:

- **Beheer van voorkeuren:** de verwerking en opslag van klantdata
- **Beheer van privacy:** het delen van klantgegevens
- **Beheer van compliance:** de toewijzing en eventuele verwijdering van persoonsgegevens

Dergelijke mogelijkheden kunnen standaard door een Customer Identity-oplossing worden aangeboden of worden geïmplementeerd via integraties met externe leveranciers die zijn gespecialiseerd in use cases op het gebied van privacy en toestemmingsbeheer.

Een goede bescherming van de privacy van gebruikers leidt tot een groter klantvertrouwen, een betere end-to-end compliance en uiteindelijk een hogere omzet.


TIP

Het valt niet mee om uw weg te vinden in het doolhof van bestaande en toekomstige complexe regels en wetten. Daarom kunt u het beste een moderne Customer Identity-oplossing gebruiken om de voorkeuren, de privacy en de compliance voor de persoonsgegevens van uw klanten centraal te beheren.

Complexiteit beheren

Organisaties krijgen vandaag de dag overal met complexiteit te maken, van het bouwen, testen en lanceren van moderne cloudnative apps voor veeleisende klanten, tot het samenvoegen of bundelen van externe en gefragmenteerde identity stores in verschillende partnerportals. Bovendien moeten de legacy producten nog steeds worden beheerd, net zolang tot de digitale transformatie van de organisatie is voltooid. Customer Identity is dus niet langer een eenvoudige oplossing waarmee klanten kunnen inloggen bij één app of website.

Maar ondanks al deze complexiteit kan Customer Identity de flexibiliteit en de groei van organisaties ondersteunen en faciliteren. Het is daarbij met name belangrijk dat een Customer Identity-oplossing de volgende mogelijkheden biedt:

- Grootschalige architecturen met meerdere organisaties ondersteunen die talloze test-, preproductie- en productieomgevingen omvatten.
- Een combinatie van moderne cloudapps en legacy on-prem producten beheren en de data gescheiden houden.
- Uitgebreide API-dekking en een intuïtief organisatiebreed beheer bieden.
- Gefragmenteerde identity-systemen op orde brengen.

IN DIT HOOFDSTUK

- **Een praktische checklist voor de implementatie van Customer Identity**
- **Identificatie van de technische en zakelijke vereisten**
- **De juiste Customer Identity-oplossing voor uw organisatie**
- **Customer Identity en doorlopende innovaties**
- **Een concurrentievoordeel creëren met een frictieloze customer experience**

Hoofdstuk 8

Tien overwegingen omtrent Customer Identity

Hier zijn tien belangrijke overwegingen om de juiste Customer Identity-oplossing voor uw organisatie te kiezen en te implementeren:

- **Evalueer de knelpunten voor uw klanten en uw interne teams.** Raken uw klanten gefrustreerd door een te lang registratieproces? Heeft u een beveiligingslek gehad? Hebben uw initiatieven voor de digitale transformatie vertraging opgelopen?
- **Definieer uw ideale customer experience.** Wat moeten uw klanten ervaren tijdens de interacties met uw merk? Wilt u een unieke login-experience in uw eigen huisstijl bieden bij de toegang tot al uw apps? Via welke kanalen wilt u deze experience bieden?

- **Bepaal de security-specificaties.** Hoe zorgt u op dit moment voor een secure access-experience? Wat wilt u in de toekomst bieden? Zijn er security- en privacywetten van kracht die u moet naleven?
- **Stel uw zakelijke doelstellingen vast.** Wat wilt u bereiken vanuit zakelijk oogpunt? Wilt u misschien naar andere landen uitbreiden of een nieuw product lanceren? Op welke termijn?
- **Zet al uw Customer Identity-behoeften op een rijtje.** Bekijk wat de meest urgente en minder urgente behoeften zijn op het gebied van user experience, security en zakelijke activiteiten. Stem vervolgens uw prioriteiten daar op af. Bespreek alles met uw interne teams en bepaal hoe eventuele tegenstrijdige belangen in evenwicht worden gebracht.
- **Weeg de opportuniteitskosten van bouwen en kopen tegen elkaar af.** Het bouwen en bijhouden van uw eigen Customer Identity-oplossing is gecompliceerd en kostbaar. U kunt uw resources beter richten op uw core business. In hoofdstuk 3 vindt u meer informatie over wat het bouwen van een eigen oplossing allemaal inhoudt.
- **Besteed Customer Identity uit aan een externe expert (zodat het goed wordt gedaan).** Bepaal met behulp van dit boek welke Customer Identity-expert bij uw organisatie past. Kies een vertrouwde partner met een bewezen reputatie die aan uw huidige en toekomstige behoeften kan voldoen.
- **Implementeer een frictieloze customer experience.** Nadat u een moderne Customer Identity-oplossing heeft gekozen, kunt u deze snel en op grote schaal implementeren in al uw klantgerichte apps, websites en portals om een frictieloze en veilige customer experience te bieden.
- **Activeer innovaties aan de hand van de Customer Identity-maturiteitscurve.** Een moderne Customer Identity-oplossing opent de deur naar een wereld boordevol kansen voor uw organisatie. Zie hoofdstuk 6 voor meer informatie over de mogelijkheden die zich in de verschillende fasen van de Customer Identity-maturiteitscurve voordoen.
- **Focus op uw concurrentievoordeel.** Met een moderne Customer Identity-oplossing kunt u zich onderscheiden van de concurrentie en een uitmuntende reputatie opbouwen op basis van vertrouwen, innovatie en een superieure customer experience voor elke gebruiker.

okta

Customer Identity. We hebben er een boek over geschreven.

bit.ly/OktaCIAudiobook

Luister nu naar het audioboek.

Veilige en frictieloze customer experiences bouwen

Als u weleens bij een website heeft ingelogd om tickets voor een concert te kopen of uw social media-account heeft gebruikt om in te loggen bij een nieuwe e-commercesite, bent u al met Customer Identity in aanraking geweest. Customer Identity voegt een digitale identity-laag toe die kan worden geïntegreerd in klantgerichte apps, websites en portals. In dit boek leggen we uit hoe u met Customer Identity uw klanten en partners veilige en frictieloze experiences kunt bieden.

In dit boek...

- De basics van Customer Identity
- Waarom Customer Identity cruciaal is
- De risico's die zijn gemoeid met het zelf ontwikkelen van een Customer Identity-oplossing
- Wat een moderne Customer Identity-oplossing precies inhoudt
- Waar u op moet letten bij een Customer Identity-oplossing
- Hoe Customer Identity op maat bijdraagt aan het succes van uw organisatie
- De toekomst van Customer Identity

okta

Lawrence C. Miller werkt al 25 jaar in de informatietechnologie en heeft meer dan 200 Voor Dummies-boeken geschreven.

Jeremie Certes is Senior Product Marketing Manager bij Okta.

Ga naar Dummies.com™
voor video's, foto-tutorials en praktische artikelen en om producten aan te schaffen.

ISBN: 978-1-394-22817-1

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.