Expertgroep

Digital Identity: the new gold

Balanceren tussen gebruikersgemak en veiligheid

shopping tomorrow

Takeaways

1. Nederlandse consumenten besteedden in 2019 voor meer dan 25,8 miljard euro aan producten en diensten via het internet. Het digitale verkoopkanaal wordt steeds belangrijker, toch kan en moet er nog veel verbeteren. Organisaties bevinden zich middenin een digitale revolutie.
2. *Customer identity and access management* (CIAM) is een uitstekend middel in de online strategie van e-commercebedrijven. Met CIAM start de gebruikersbeleving in een veilige, eenvoudig te gebruiken en privacy-vriendelijke omgeving.
3. Uit onderzoek van Okta blijkt dat Nederlanders gemiddeld negen wachtwoorden moeten onthouden in het dagelijkse leven, en dat ze er maandelijks gemiddeld drie vergeten. De praktijk leert dat een moeizame login leidt tot afname van gebruik en daarmee omzet.

Host

okta

Voorzitter

IDentity•Next

Customer identity als basis voor de digitale koers?

De online consumentenbestedingen in de detailhandel groeien dit jaar sterk, wijzen cijfers van het CBS uit.[1] De situatie rondom COVID-19 speelt hierin een belangrijke rol. Als gevolg van deze groei zijn de eisen aan online winkelen hoger geworden. De consument verwacht meer en meer van de online retailer, voornamelijk op het vlak van gebruikerservaring, merkbelofte en service: de zogenoemde 'customer experience'. Anno 2020 moet winkelen voornamelijk eenvoudig en persoonlijk zijn. Daarbij switcht de consument eenvoudig tussen de verschillende on- en offlinekanalen, in alle fasen van de klantreis: vanaf het moment dat hij iets bekijkt, tot aan de geboden service na aanschaf en alles daartussenin.

Consumenten zijn zich vaak niet bewust van het digitale spoor dat ze online achterlaten en ze denken beschermd te zijn tegen fraude en datalekken. Ze verwachten van organisaties dat hun privacy gewaarborgd wordt volgens de gestelde wet- en regelgeving. Dit blijkt in de praktijk lastig voor bedrijven, die zoeken naar de optimale balans tussen gebruiksvriendelijkheid en beveiliging. Bij het zoeken naar deze balans wordt de term *customer identity and access management* veel gebruikt, kortweg CIAM. Deze term is niet voor iedereen even bekend, toch heeft bijna iedereen ermee te maken.

De meeste Nederlanders hebben meerdere inloggegevens, zowel zakelijk als privé. Hiermee doen zij bijvoorbeeld een aankoop in een webshop, declareren ze nota's bij verzekeraars of loggen ze in om online te bankieren. Dit zijn allemaal voorbeelden waarin digitale toegang wordt verstrekt, oftewel vormen van CIAM. Alle organisaties met een mogelijkheid voor eindgebruikers om in te loggen hebben te maken met CIAM, hetzelfde geldt voor die eindgebruikers.

Customer identity and access management
Customer identity and access management (CIAM) is een cruciaal onderdeel van online strategie. Het draait om de verlening van toegang aan de juiste individuele consument, tot de juiste bronnen, op het juiste moment, om de juiste redenen.[2] De klantervaring verbetert doordat de toegang tot de benodigde applicaties en diensten goed wordt beheerd en beveiligd, net als de data van de klant en de organisatie. Hierbij is elke organisatie op zoek naar de optimale balans tussen ten eerste veiligheid, ten tweede gebruiksvriendelijkheid en ten derde het verzamelen van klantgegevens. Op alle drie is wet- en regelgeving van toepassing.

1 *CORONACRISIS JAAGT ONLINE WINKELEN AAN IN HET TWEEDE KWARTAAL*, CBS, 4 AUGUSTUS 2020, WWW.CBS.NL/NL-NL/NIEUWS/2020/32/CORONACRISIS-JAAGT-ONLINE-WINKELEN-AAN-IN-HET-TWEEDE-KWARTAAL

In deze bluepaper heeft onze expertgroep zich de vraag gesteld of *customer identity* het nieuwe goud is. De manier van toegang verlenen binnen CIAM staat hierin centraal. De expertgroep heeft zich vooral gericht op de vraag of customer identity de basis van de nieuwe digitale koers voor organisaties moet zijn. Hoe sluit dit dan vervolgens aan op de missie, visie en strategie van een organisatie? Welke use cases zijn van toepassing voor een succesvolle strategie binnen de verschillende domeinen b2b, b2c en b2e (business-to-employee)? Dit alles hebben de experts in de context geplaatst van gebruiksvriendelijkheid en van veiligheid, om zo een gerichte aanzet te geven tot een succesvolle integratie van CIAM in de digitale koers van organisaties.

1. Hoe vaar je een succesvolle digitale koers?

Vandaag de dag staan bedrijven onder druk om hun bedrijfsmodellen steeds verder te ontwikkelen, in reactie op nieuwe gedragspatronen en snelle veranderingen in het concurrentielandschap. Dit kan worden omschreven als de opkomst van de '*overwhelming digital condition*', de noodzaak tot digitalisering. De meeste bedrijven hebben digitale transformatie tot prioriteit gemaakt, mede gestimuleerd door COVID-19. Toch ontbreekt het bij sommige organisaties nog aan toewijding.

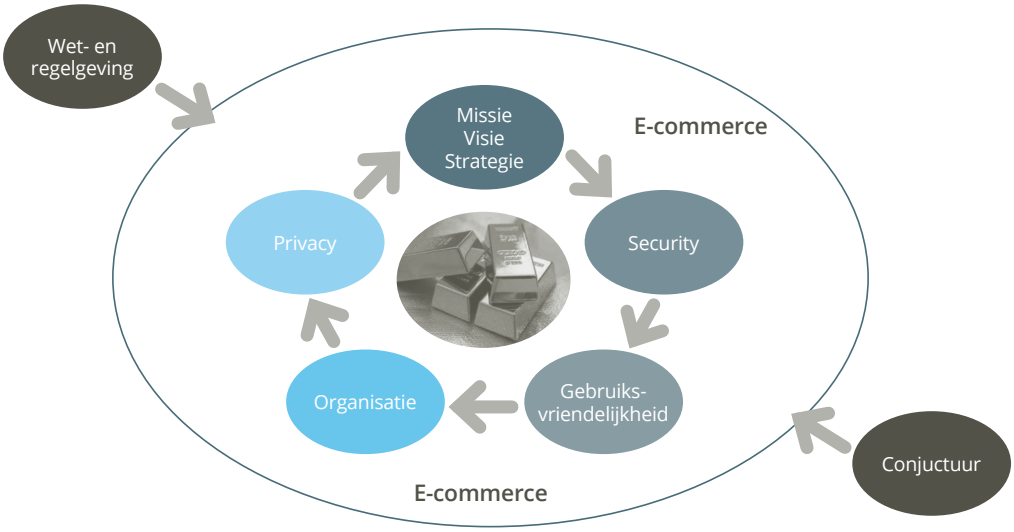
De simpele vraag 'Wie moet toegang krijgen tot of binnen mijn organisatie?' is in steeds complexer aan het worden. Bedrijven en organisaties zijn dynamischer dan ooit, ze veranderen en ontwikkelen zich steeds sneller. De behoeften aan softwareapplicaties en systemen groeien mee met de behoeften van consumenten, partners of medewerkers. Binnen al die veranderingen en ontwikkelingen zien we meer uitdagingen en risico's voor de consument die hier doorheen navigeert.

1.1 Missie – visie – strategie

Automatisering biedt een deel van de oplossing om tot een verantwoord systeem van beveiligde toegang te komen. Toch is techniek slechts een onderdeel van CIAM, aangezien het meer omvat dan ict-beslissingen. Het begint bij de bovenkant van een organisatie: de missie, visie en strategie van een bedrijf moeten een directe aanleiding geven om CIAM te willen implementeren. Om dit te realiseren moeten organisaties duidelijk krijgen hoe ze CIAM kunnen toepassen voor een succesvolle online strategie.

Authenticatie is vaak het eerste 'contactpunt' tussen een organisatie en een consument of medewerker. Als CIAM correct is geïmplementeerd, wordt het door meer eindgebruikers toegepast, wat de bedrijfsreputatie verbetert en de omzet verhoogt. Als dit daarentegen verkeerd wordt uitgevoerd, dan zal het bedrijf hieronder lijden; een consument zal een transactie niet afmaken of zelfs naar een andere aanbieder gaan. De schade bij medewerkers ligt veel meer in het onbedoeld lekken van persoonlijke of bedrijfsinformatie en de bijbehorende financiële en reputatieschade.

2 'IDENTITY AND ACCESS MANAGEMENT IS THE DISCIPLINE THAT ENABLES THE RIGHT INDIVIDUALS TO ACCESS THE RIGHT RESOURCES AT THE RIGHT TIMES FOR THE RIGHT REASONS', GARTNER GLOSSARY, GERAADPLEEGD OP 18 OKTOBER 2020, WWW.GARTNER.COM/EN/INFORMATION-TECHNOLOGY/GLOSSARY/CUSTOMER-IDENTITY-ACCESS-MANAGEMENT-CIAM



Kritische succesfactoren voor digitale strategie

In het begrip CIAM worden aspecten verenigd die veelal als strijdig met elkaar worden gezien. Hierbij zijn de volgende waarden van belang:

- gebruiksvriendelijkheid en -gemak zullen altijd leidend zijn in het menselijk handelen, ondanks de risico's die daaraan verbonden zijn;
- technologische ontwikkelingen gaan altijd sneller dan de ontwikkeling van toezicht en beleid;
- het beheer en gebruik van een digitale identiteit moet met (meer) beveiliging gepaard gaan.

Deze punten brengen ons bij de kernvraag: wat zijn de kritische succesfactoren voor een succesvolle digitale koers die is gebaseerd op CIAM?

1.2 Breng mensen, processen en technologieën samen

Het combineren van medewerkers die werkzaam zijn in meerdere disciplines en met verschillende processen en technologieën is essentieel voor het opzetten van nieuwe bedrijfsmodellen en diensten. Hierdoor leren werknemers nieuwe vaardigheden en kunnen verschillende disciplines samenwerken voor een succesvolle (online) strategie.

Samenwerken is in elke organisatie essentieel: binnen een afdeling, met collega's van andere afdelingen of met mensen die deel uitmaken van andere organisaties. Hoe kan een bedrijf ervoor zorgen dat al die professionals efficiënt en veilig kunnen samenwerken en dat zij beschikken over de benodigde informatie om de gestelde doelen te bereiken?

1.3 Formuleer een heldere strategie

Een (online) strategie vergt organisatorische verandering en geduld. De organisatiestructuur moet worden omgegooid en de juiste platformen moeten op maat worden gemaakt. Hiervoor is een duidelijke platformstrategie nodig, die continue veranderingen ondersteunt.

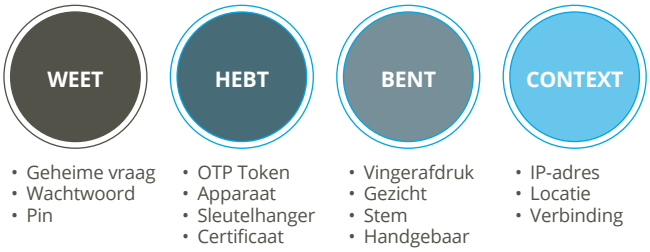
1.4 Tooling

Een strategie moet geen doel op zich zijn: het succes van een strategie valt of staat bij de juiste executie, waarvoor tooling essentieel is. Op het gebied van CIAM zijn er vele tools en platformen die de strategie kunnen ondersteunen.

Veilige toegang volgt uit een combinatie van deze factoren:

- iets wat je weet
- iets wat je hebt
- iets wat je bent
- de context waarin je je bevindt

Toegang krijgen begint niet altijd bij 'iets wat je weet'. Het geven van toegang kan juist vereenvoudigd worden door andere onderdelen te combineren. Als een persoon zich met een telefoon op een bepaalde locatie bevindt, dan is toegang zonder wachtwoord mogelijk. Hierbij geven de onderdelen 'context' en 'iets hebben' voldoende zekerheid voor het gevraagde toegangsniveau.



Factoren voor veilige toegang en bijbehorende voorbeelden

2. De context van CIAM

In de klantgerichte wereld van vandaag verwacht een gebruiker veilige en laagdrempelige toegang. CIAM maakt het mogelijk om snel, veilig en frictieloos vanaf waar dan ook, wanneer dan ook, en op welk apparaat dan ook de juiste toegang tot gewenste informatie te ontvangen.

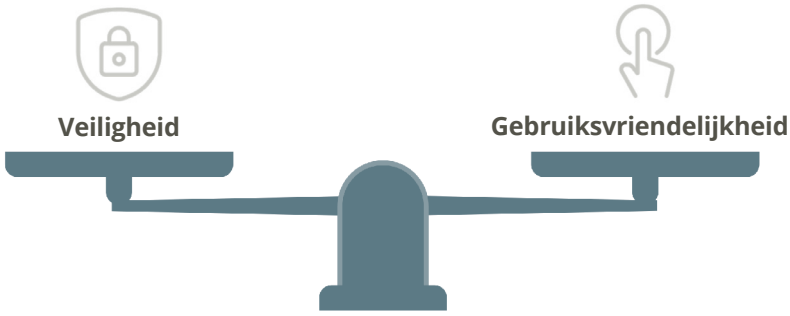
2.1 Identity en access management voor medewerker en consument

Al decennialang zetten organisaties identiteit in om de juiste personen toegang te geven tot de juiste applicaties en data. Medewerkers identificeren zich binnen het interne systeem voor identity access management (IAM), dat vervolgens zorgt voor de veilige validatie waarmee personen kunnen aantonen dat ze daadwerkelijk zijn wie ze zeggen te zijn. CIAM is een essentieel onderdeel van de IAM-strategie van een organisatie. Het grote verschil tussen CIAM en interne IAM is dat CIAM met name is gericht op de buitenwereld en IAM op medewerkers. Daarbij hoort een belangrijk verschil in benadering: eindgebruikers hebben andere behoeften en hebben niet te maken met intern gestelde richtlijnen. Eindgebruikers krijgen ook geen 'security awareness'-training voor het aanschaffen van een paar sneakers. Hierbij is het belangrijk te onthouden dat het medewerkers zijn die toegang hebben tot customer identities ofwel 'het goud'. Denk aan medewerkers in marketing, finance en sales. Dit maakt interne IAM zeer relevant voor de vraag of CIAM het nieuwe goud is, en hoe dit goud moet worden beveiligd.

TIP!
Eindgebruikers kunnen voorgoed verdwijnen als processen zoals registratie, inlog en gegevensbescherming negatieve ervaringen opleveren. Zorg er dus voor dat je eindgebruikers een positieve ervaring hebben, waardoor hun loyaliteit toeneemt.

2.2 Gebruiksvriendelijkheid versus veiligheid

Veiligheid en gebruiksgemak worden vaak in een weegschaal afgebeeld. Als het een toeneemt, neemt het ander gelijkmatig af. Technologie brengt de wegschaal regelmatig in onbalans, wat zorgt voor kansen. Voorbeelden hiervan zijn de introductie van bijvoorbeeld vingerafdruklezers op Mac-producten en Face ID in Windows 10. Hierdoor krijgen gebruikers toegang tot laagdrempelige biometrische authenticatie.



Zoeken naar balans

De waarde van wat er beveiligd moet worden, speelt een belangrijke rol bij het inrichten van veiligheid, waarbij waarde een ruim begrip is. Reputatieschade wordt bijvoorbeeld in eerste instantie niet als financiële kwestie gezien, totdat de gevolgen op de lange termijn zichtbaar worden.

TIP!
De balans tussen veiligheid en gebruiksgemak is afhankelijk van het risicoprofiel. Bij een hoog risicoprofiel zet je meer authenticatiefactoren in, terwijl je bij een laag risicoprofiel juist de focus op snel inloggen en lagere veiligheid legt. Op die manier kun je als bedrijf balanceren tussen gemak en beveiliging, per organisatielaag.

2.3 Digitale identiteit

Digitale identiteit is van belang in de werksfeer, maar ook privé heeft men steeds meer digitale identiteiten zoals blijkt uit onderzoek van Okta.[3] De verstrekte gegevens bij deze identiteiten zijn steeds sterker gedistribueerd, waardoor de eigenaar minder zicht heeft op de locatie van de data. Dit wordt nog ingewikkelder naarmate privé- en zakelijke identiteiten steeds meer door elkaar heen lopen. Er wordt vaker thuis gewerkt, tijdens en buiten kantooruren, waardoor de werklaptop sneller gebruikt kan worden door ongenode bezoekers, of onwetende huisgenoten met de beste bedoelingen. Ook raken zakelijke en particuliere inlogaccounts op apparaten steeds meer verweven, denk bijvoorbeeld aan het gebruik van Gmail voor zowel werk als privé, toegankelijk via dezelfde omgeving.

3 *EEN TOEKOMST ZONDER WACHTWOORDEN*, OKTA, JUNI 2019, WWW.OKTA.COM/NL/RESOURCES/WHITEPAPER-PASSWORDLESS-FUTURE

Steeds vaker gebruiken organisaties sociale inlogmogelijkheden: bij de KvK kan men op het forum voor ondernemers inloggen met een Facebook-identiteit. Hoeveel ondernemers zouden weten dat ze hiermee ongemerkt de optie 'apps' activeren, waarmee zij de KvK het recht geven om hun profielgegevens van Facebook te importeren? Hierbij is een duidelijk keuze gemaakt voor gebruiksvriendelijkheid boven veiligheid.

2.4 Flexibiliteit

Veel medewerkers gebruiken naast een door de werkgever verstrekt apparaat ook een eigen device, zoals een laptop, telefoon of tablet. Dit principe van '*bring your own device*' geldt in bijna elke organisatie. Een organisatie kan ervoor kiezen om ook vanaf een 'onbeheerd device' meerdere authenticatiefactoren te vragen als iemand een interne applicatie wil benaderen. Ook consumenten kunnen dit ervaren, bijvoorbeeld bij internetbankieren. Om toegang tot een bankrekening te krijgen zijn meer gegevens nodig dan een login via sociale media. Dit is anders dan het achterlaten van een reactie bij een blog, dat zonder beveiliging mogelijk is. De flexibiliteit van het autorisatieproces is dus afhankelijk van de data waar een entree voor wordt gevraagd. Is de waarde hoog en de informatie vertrouwelijk, dan zal de consument via verschillende factoren moeten bewijzen dat hij is wie hij zegt te zijn.

2.5 Beheer van CIAM

Goede CIAM-oplossingen faciliteren het opbouwen en beheren van uniforme online gebruikersprofielen. Ze laten zich vergelijken met de goudreserves bij Fort Knox, zo belangrijk zijn de data voor organisaties. Er zijn tools beschikbaar voor registratie, (*single sign-on*) login en toegangsbeheer, met voorkeursinstellingen om accounts te configureren, waarbij eindgebruikers uiteindelijk zelf hun identiteitsgegevens kunnen bijwerken. Schaalbaarheid en flexibiliteit zijn nodig om pieken op te vangen, bijvoorbeeld als gevolg van reclameacties en seizoensgebonden promoties.

2.6 Privacy by design

'Privacy by design' is een veelvoorkomende trend binnen organisaties. Dit betekent dat systemen en procedures vanaf het begin worden ontworpen met privacy als leidraad. Dit is essentieel, want gegevens van consumenten en medewerkers worden binnen verschillende lagen van de organisatie vastgelegd. De manier van vastleggen is belangrijk, aangezien het gaat om bescherming tegen fraude en andere cyberrisico's. Het zorgt er ook voor dat de Algemene Verordening Gegevensbescherming[4] wordt nageleefd.

TIP!
Als privacyadviseur moet je net zoals marketing- en ict -afdelingen verantwoordelijkheid pakken op het gebied van customer identity.

4 SINDS 25 MEI 2018 IS DE ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG) VAN TOEPASSING, WAARMEE IN DE HELE EUROPESE UNIE DEZELFDE PRIVACYWETGEVING GELDT (BRON: AUTORITEIT PERSOONSGEGEVENS, WWW.AUTORITEITPERSOONSGEGEVENS.NL/NL/ONDERWERPEN/ALGEMENE-INFORMATIE-AVG/ALGEMENE-INFORMATIE-AVG)

3. De beste online strategie?

CIAM maakt het mogelijk om de gegenereerde customer identity-data te gebruiken om klanten beter te leren 'begrijpen', het productaanbod relevanter te maken en services beter te kunnen afstemmen op eindgebruikers. Het resultaat is een duidelijke online strategie en een gevoel van veiligheid bij de eindgebruiker. De rol, het gebruik en de functionaliteit van een CIAM-platform kent vele aspecten. Een aantal daarvan kan door consumenten als negatief worden gezien. Toestemming voor de inzet ervan, in overeenstemming met de AVG, is essentieel.

Centraal bij CIAM staat de vraag hoe toegang wordt verkregen tot customer identity-data. Dit is sterk afhankelijk van het perspectief achter de vraag in een concreet geval. Er spelen aspecten rondom gebruiksvriendelijkheid (het gemak waarmee toegang wordt verkregen), toegankelijkheid (de mate waarin iemand met een beperking toegang kan krijgen) en snelheid (de tijd tussen 'ik wil' en 'ik kan').

Authenticatie, waarbij wordt nagegaan of een gebruiker is wie hij beweert te zijn, is van groot belang. Vaak gebeurt dat aan de hand van een gebruikersnaam en een wachtwoord. In de loop van de tijd zijn er echter veel manieren ontwikkeld om dit proces gemakkelijker en veiliger te maken. Dit komt voornamelijk tot uiting in de diverse manieren waarop een gebruiker moet bewijzen dat hij is wie hij zegt te zijn.

Niet alle authenticatiefactoren zijn geschikt voor de online strategie die een organisatie kiest. Zo is het in b2e zeer ongebruikelijk om social log-in (het inloggen van medewerkers via een social-account zoals Facebook) in te zetten. Ook is het bijvoorbeeld zeer ongebruikelijk om consumenten in een b2c-webwinkel te laten inloggen met een digitale identiteit die behoort tot de werkgever, terwijl die zakelijke identiteit in b2b-omgevingen juist uitkomst biedt.

Factoren voor veilige toegang

Vaak denkt men alleen aan zogenoemde multifactorauthenticatie om gebruikers te verifiëren aan de hand van meer dan één manier. Toch kan een enkel middel ook meerdere factoren bewijzen, wat frictie enorm kan beperken. FIDO[5], een alliantie met als doel standaarden te ontwikkelen die het aantal wachtwoorden verminderen, heeft sinds 2018 een certificering die de veiligheid van middelen aantoont. Met deze standaard zijn gemak en veiligheid verenigd.

3.1 Wat is de rol van interne IAM?

Interne IAM speelt een belangrijke rol bij de online strategie van organisaties. Dit geldt bijvoorbeeld voor interne medewerkers die in vaste dienst zijn, maar ook voor externen, partners, consultants of tijdelijke projectgroepen. Al deze doelgroepen moeten, om efficiënt hun werk te kunnen doen, tijdig toegang hebben tot de juiste platformen, applicaties of systemen. Snel handelen is hierbij essentieel. Daarnaast gaat het ook om precisie; het is onwenselijk dat verkeerde rechten aan een intern (of

5 DE FIDO ALLIANCE IS EEN OPEN BRANCHEVERENIGING DIE IN FEBRUARI 2013 IS OPGERICHT EN DIE ALS MISSIE HEEFT HET ONTWIKKELEN EN PROMOTEN VAN AUTHENTICATIESTANDAARDEN DIE DE OVERMATIGE AFHANKELIJKHEID VAN WACHTWOORDEN IN DE WERELD HELPEN VERMINDEREN. (BRON: WIKIPEDIA)

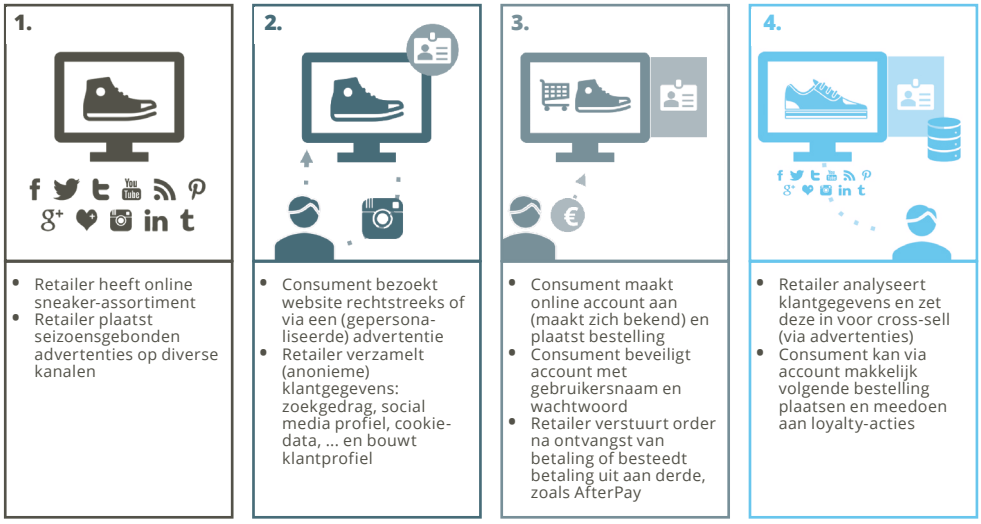
extern) persoon worden toegekend. Ook het behoud van rechten bij uitdiensttreding kan lastige situaties opleveren. Bijvoorbeeld wanneer een werknemer die naar de concurrent vertrekt, nog steeds toegang heeft tot zijn oude e-mail met financiële en strategische updates. Kortom: voor organisaties is het beheer van digitale identiteiten en toegang tot klantdata erg belangrijk.

Use case business-to-employee
Het is een bekend fenomeen: een medewerker komt nieuw in dienst en kan niet wachten om aan de slag te gaan en zichzelf te bewijzen. Na de eerste kennismaking met het nieuwe team is het tijd om te starten en te laten zien wat hij allemaal in huis heeft. Helaas is de juiste toegang tot applicaties en systemen vaak nog niet geregeld. Zelfs de mail doet het niet. Erg frustrerend, het is geen uitzondering dat de juiste toegang pas na een week is geregeld. Vervelend natuurlijk voor het bedrijf dat er een week verloren gaat. Maar wat waarschijnlijk zwaarder weegt, is de aanslag op de motivatie van de nieuwe medewerker. Hij stond immers te popelen om zichzelf aan het nieuwe team te bewijzen. Het komt voor dat de identiteit van een medewerker nog niet geactiveerd is op het moment dat hij in de nieuwe rol start. Dit is zeer kostbaar voor het bedrijf, omdat hij niet direct aan de slag kan. Vaak worden dan noodprocedures opgestart, wat bij de ondersteunende afdeling weer ten koste van andere werkzaamheden gaat.
Ook het proces rondom uitdiensttreding van medewerkers is van belang. Het is onder andere vanuit security-oogpunt belangrijk om rechten in te trekken van medewerkers die uit dienst gaan, zodat er geen misbruik meer van kan worden gemaakt.

3.2 Wie heeft er toegang tot customer identity-data?

Bij sommige organisaties krijgen werknemers zonder controle of verificatie direct toegang tot alle informatiebronnen van het bedrijf. In andere bedrijven is de toegang tot informatie zo geminimaliseerd dat er mogelijk kansen gemist worden voor het effectief benutten van data.

Bij toegang tot e-commerceplatformen ontstaat er een directe relatie tussen de consument en de aanbieder. Dat komt doordat de eindgebruiker via tal van systemen informatie moet opgeven. De kans bestaat echter dat de aanbieder deze gegevens koppelt aan instanties die zaken als kredietwaardigheid checken. Hierdoor zijn er derde partijen betrokken die de customer identity-data aanvullen, zonder dat de consument daar in eerste instantie iets van merkt.



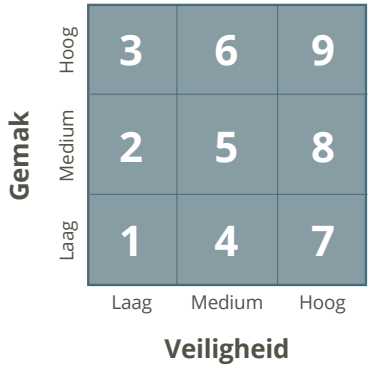
CIAM in de praktijk

3.3 Hoe gemakkelijk krijg je toegang?

Voor ieder bedrijf moet de balans worden opgemaakt tussen veiligheid en gebruikersgemak. Een organisatie heeft natuurlijk belang bij gegevens die zo veilig mogelijk zijn, terwijl een medewerker of consument liever zo snel mogelijk wil inloggen, met persoonlijke data die alleen voor hem bestemd zijn. Snelheid wordt vaak genoemd als sleutelelement; als het inloggen te lang duurt en te complex is, gaat men op zoek naar andere wegen. De gemaksvraag is daarom een hele belangrijke.

Mensen moeten nu eenmaal aantonen dat ze zijn wie ze zeggen dat ze zijn. In het echt herkennen mensen elkaar, maar via een pc is dat voor een bedrijf lastiger. Hoe weet je zeker dat jouw laptop niet is uitgeleend aan je buurman?

Deze balans vergt een samenspel tussen organisaties, medewerkers en consumenten en is bovendien contextafhankelijk. In sommige gevallen is een strenge en veilige methode logischerwijs vereist, waarbij op gebruiksgemak ingeleverd dient te worden. Terwijl andersom hetzelfde geldt; voor data met een laag risicoprofiel zal iedereen begrijpen dat gemak belangrijker is dan beveiliging.



9	Gebruikersnaam, ingebouwde biometrie en eenmalig push-verzoek (ja/nee)
8	Gebruikersnaam, ingebouwde biometrie en fysiek token
7	Gebruikersnaam, fysiek token en eenmalig push-verzoek (ja/nee)
6	Gebruikersnaam en ingebouwde biometrie
5	Gebruikersnaam en OTP-push (one-time password) via app
4	Gebruikersnaam en fysiek token
3	Gebruikersnaam en pincode
2	Gebruikersnaam en wachtwoord
1	Gebruikersnaam en eenmalig nummer via sms/app/e-mail

Verschillende vormen van authenticatie, gescoord op veiligheid en gemak

3.4 Hoe veilig zijn customer identity-data?

Veiligheid is een van de belangrijkste redenen om extra aandacht te besteden aan customer identity. Voor de authenticatie van gebruikers kan een veilige inlogomgeving worden gecreëerd. Verreweg de meeste hacks bij bedrijven zijn te herleiden tot het (her)gebruik van zwakke wachtwoorden en/of inloggegevens.[6] In een juist ingerichte omgeving is het mogelijk om identiteiten te koppelen aan rollen binnen een bedrijf, zodat acties traceerbaar zijn. Daarnaast is het ook voor werknemers zelf belangrijk te weten dat hun data op een juiste en veilige manier worden behandeld.

3.5 Hoe beveilig je digital identity-data?

Een eindgebruiker is zelf niet verantwoordelijk voor de beveiliging van zijn digitale identiteit. Of toch wel? Er is wel degelijk individuele verantwoordelijkheid. Daarbij hoort het maken van de juiste afweging tussen gemak en veiligheid, zoals wanneer je als werknemer gebruikmaakt van een applicatie waar je geen toestemming van de ict-afdeling voor hoeft aan te vragen. Bedenk daarnaast bijvoorbeeld dat het doorgaans ongewenst is om gebruik te maken van de digitale identiteit van een collega die meer informatie tot zijn beschikking heeft dan jijzelf. De gebruiker is dus verantwoordelijk voor veilig gebruik.

Use case business-to-business

Customer identity and access management speelt in b2b bijvoorbeeld bij de bediening van adviseurs van een verzekeringmaatschappij. Een adviseur logt in op de partneromgeving van de verzekeraar, wordt herkend en krijgt gepersonaliseerd toegang om bijvoorbeeld schadediensten af te nemen. Deze zijn toegankelijk via meerdere applicaties die zijn aangesloten op een platform. Om toegang te krijgen tot het digitale platform is er een samenwerkingsovereenkomst met de verzekeraar.

Doelstelling vanuit klantbedieningsperspectief is om single sign-on (SSO), één login voor alle productapplicaties, te realiseren. Doel is van een versnipperde naar een geïntegreerde customer journey te bewegen, met een juiste balans tussen veiligheid en gebruiksgemak.

Het niveau van de beveiliging hangt hierbij sterk af van het product dat afgenomen wordt en de data die daarbij worden verwerkt. Het minimale niveau van beveiliging is multifactorauthenticatie.

Een interessante ontwikkeling die versnelling aanbrengt in SSO-klantbediening voor verzekeraars is eHerkenning. In essentie regelt eHerkenning de digitale herkenning (authenticatie) en controleert het de digitale bevoegdheid (autorisatie) van iemand die online een dienst wil afnemen. Het is de vervanger van het digitale paspoort, dat niet meer voldoet aan de hedendaagse veiligheidseisen.

Een andere ontwikkeling is de toename van directe integraties tussen de interne IAM-systemen van bedrijven. Hiermee vervallen de afhankelijkheid van eHerkenning en de kosten van uitgifte van identiteiten. Ook is integratie vaak sneller dankzij wereldwijd geadopteerde standaarden als SAML (Security Assertion Markup Language) en OIDC (OpenID Connect).

6 *COMPROMISED CREDENTIALS: THE PRIMARY POINT OF ATTACK FOR DATA BREACHES*, SECURITYWEEK, 24 JANUARI 2018, WWW.SECURITYWEEK.COM/COMPROMISED-CREDENTIALS-PRIMARY-POINT-ATTACK-DATA-BREACHES

3.6 Wat is de waarde van digital identity?

De customer of employee identity is zeer waardevol. Het is de toegangspoort voor een consument of een medewerker naar relevante informatie. Zonder deze identiteit is het anno 2020 onmogelijk om online actief te zijn.

De waarde van de gebruikte identiteit is erg afhankelijk van de methoden die door een organisatie worden ingezet. De bronnen van de methoden zijn hierin leidend. Zo kan via iDIN[7] gebruik worden gemaakt van de databases van een bank waardoor de data hoogwaardig is. Met iDIN kan een eindgebruiker zijn identiteit online bevestigen, omdat hij zich al heeft gelegitimeerd bij het openen van een bankrekening. Daarnaast biedt het bedrijven bescherming tegen identiteitsfraude, door fraudemonitoring van de banken.

4. Conclusie en praktische tips

Gesteld kan worden dat CIAM essentieel is voor een naadloze digitale gebruikerservaring, en dat gebruikersdata het nieuwe goud zijn. Zoals besproken is een juiste balans noodzakelijk: te veel nadruk op authenticatiebeveiliging kan leiden tot het afhaken van eindgebruikers. Een gebruiker wil niet als potentiële fraudeur worden behandeld. De verzameling van gebruikersgegevens biedt voordelen voor marketing- en verkoopafdelingen.

Organisaties moeten zich er bij de toepassing van CIAM van bewust zijn dat gegevens van eindgebruikers persoonlijk identificeerbare informatie bevatten, die onderhevig zijn aan een grote en groeiende verscheidenheid aan voorschriften en privacywetten. Regelgeving en privacywetten vergroten de complexiteit van een CIAM-strategie enorm. Binnen deze grenzen moeten organisaties een manier vinden om te zorgen voor volledige naleving en om datalekkage en mogelijke reputatie-schade te voorkomen.

De volgende praktische tips kunnen organisaties verder op weg helpen met CIAM, om te komen tot een succesvolle digitale strategie.

1. Een succesvolle online strategie is een integraal onderdeel van de overkoepelende missie, visie en strategie van een bedrijf. Probeer vanuit de wensen en mogelijkheden van de identiteit (klant, leverancier, werknemer) te denken. De techniek kan aangepast worden aan deze keuzen.
2. Verdiep je in (interne) klanten en bouw een vertrouwensrelatie op. Met deze informatie kun je de juiste keuzen maken en deze waar nodig bijsturen om tot het maximale resultaat te komen.
3. Zorg voor de optimale balans tussen gebruikservaring en veiligheid. Het overzicht van beschikbare factoren in deze bluepaper kan nieuwe inzichten geven voor de eerste verbeterstap.
4. Integreer privacy by design als aanzet voor het gebruik van technologie en processen.
5. Het betrekken van stakeholders binnen elke laag van een organisatie is belangrijk om customer identity and access management succesvol te implementeren.
6. Digitale identiteiten zijn de kroonjuwelen van de organisatie. Ga hier zorgvuldig mee om en bewaak ze met verve.

7 *IDIN* IS EEN NEDERLANDS ONLINE IDENTIFICATIEMIDDEL. DE 'ID' STAAT VOOR IDENTIFICEREN EN 'IN' STAAT VOOR INLOGGEN. HIERMEE KUNNEN CONSUMENTEN ZICH BIJ ANDERE ORGANISATIES ONLINE IDENTIFICEREN, MET DE VEILIGE EN VERTROUWDE INLOGMIDDELEN VAN HUN EIGEN BANK. ZIE WWW.IDIN.NL

HOSTS

Anke Massaro
Account Executive
Okta UK Limited

VOORZITTER

Robert Garskamp
Founder
Identity.Next

Leden expertgroep

Ali Babakhan
Product Manager Rabo eBusiness
Rabobank Nederland

Annette Poiesz
CEO
The Chain Never Stops B.V.

Berber Merx - Rienks
Director Digital Customer
PwC

Frank Benus
Regional Principal Platform Specialist
Okta UK Limited

Jeanette van Sommeren
Head of IT & Innovation
Makro Nederland

Jesper Elders
Online Marketing Manager
Decathlon Nederland

Jochem Boot
Head of Digital Transformation
De Mandemakers Groep

Joost van der Wal
Architect Applicaties & Data analytics
Detailresult Groep

Koen Oud
Sales Executive
FuseLogic B.V.

Maarten Bevers
Lead Global Support Office & Netherlands
Ahold Delhaize

Margot Markhorst
Product Consultant
Currence

Maurice van Franck
Directeur
TopShoe.nl

Monique van Hal
Brand & Customer Experience manager
Cavalor

Peter Eikelboom
Innovatie Manager
De Volksbank N.V.

Philip Kurtin
Founder & CEO
eigenlinks BV

Pjotr van Amelsfoort
Product Owner Digital
Centraal Beheer Bedrijven

Rick Maresch
Head of Digital Transformation
TCXA