CIAM vs. IAM:

Por que os IAMs tradicionais não devem ser usados para clientes

Compreensão das diferenças entre CIAM e IAM

A identidade digital está no centro da transformação digital de todas as empresas. O valor dos dados do perfil dos clientes que está vinculado às identidades deles cresceu drasticamente e agora é um fator crucial de sucesso para muitas empresas. Ele forma a base para analisar, compreender e prever o comportamento do consumidor e as jornadas do cliente, desde o primeiro contato até as decisões de compra e fidelidade à marca a longo prazo.

É um equívoco comum que a tecnologia exigida para o Customer Identity and Access Management (CIAM) seja a mesma para o Identity Access Management (IAM) tradicional. As soluções tradicionais de IAM, também chamadas de IAM de empresas, funcionários ou força de trabalho, são os sistemas de TI que garantem que apenas a força de trabalho ou os parceiros de negócios conhecidos de uma empresa possam acessar a rede corporativa e seus recursos.

O IAM tradicional é normalmente bem estabelecido, levando algumas empresas a assumirem a suposição equivocada de "como já temos essa tecnologia internamente, não pode ser tão difícil estendê-la aos nossos clientes". Na raiz dessa abordagem está uma drástica depreciação das diferenças entre o IAM da força de trabalho e o IAM do cliente, e a complexidade do gerenciamento das identidades dos clientes para as propriedades digitais voltadas para o público de uma empresa. O CIAM tem requisitos diferentes, e muito mais desafiadores, do que o IAM da força de trabalho; Como resultado, a reutilização das soluções de IAM da força de trabalho pode ser uma abordagem problemática.

Um IAM tradicional não consegue fornecer insights sobre quem é um usuário, as ações que ele realiza ou o que influencia seu comportamento digital.

Reutilizar o IAM tradicional para o CIAM não é a resposta

Como o IAM tradicional foi projetado para facilitar o acesso dos funcionários aos sistemas internos, ele não consegue fornecer insights sobre quem é um usuário. De fato, a identidade é assumida, e não é possível rastrear os dados avançados (como as ações que um usuário realiza e o que influencia sua jornada e comportamento na esfera digital). Mas as empresas exigem esses tipos de dados para entender seus clientes e competir no mercado digital.

Além disso, em muitas das maiores corporações, sistemas tradicionais de IAM podem ser responsáveis por administrar até dezenas de milhares de identidades de funcionários. Mas marcas de alto volume precisam lidar com dezenas, ou até centenas, de *milhões* de contas de clientes simultaneamente. E os consumidores modernos esperam atrito zero. Uma solução de identidade precisa ser dimensionada para "fora" e "para cima" para atender a essa carga de trabalho com pouca ou nenhuma latência perceptível.

Um estudo recente da Akamai descobriu que um atraso de dois segundos no tempo de carregamento da página da Web aumenta as taxas de rejeição em 103%, e 53% dos visitantes do website para dispositivos móveis abandonarão uma página que leva mais de três segundos para carregar.[1] Portanto, se o sistema de gerenciamento de identidades falhar, ou ficar lento porque não consegue lidar com a carga, suas taxas de conversão e receita provavelmente serão afetadas. Ironicamente, os picos de carga e o aumento do tráfego de clientes são normalmente causados por campanhas bem-sucedidas, o que significa que um sistema de gerenciamento de identidades lento está trabalhando ativamente contra esforços comerciais deliberados e de difícil concorrência.

> *Um sistema lento de gerenciamento de identidades atua ativamente contra os esforços deliberados e árduos de negócios.*

Plataformas de CIAM dedicadas, como a Akamai Identity Cloud, foram projetadas para fornecer às empresas o valor máximo dos dados de perfil do cliente. Soluções como essa oferecem experiências de cliente sem interrupções e sem fricção, para que tarefas como login, autenticação ou gerenciamento de preferências não impeçam a atividade. Além disso, as tecnologias de CIAM atendem à necessidade crítica de proteger dados pessoais em redes públicas, além de permitir que empresas globais obedeçam a diversas regulamentações de privacidade e que mudam com frequência.

A tabela a seguir descreve as principais diferenças entre o IAM tradicional e o CIAM e suas aplicações.

IAM TRADICIONAL	IAM DO CLIENTE
Gerenciar **a identidade do funcionário** dentro de uma corporação.	Gerenciar **a identidade do cliente** em websites multicanais digitais voltados para o cliente (Web, dispositivos móveis, IoT).
Os usuários são **registrados por suas empresas,** com os principais dados de perfil sendo preenchidos pelo RH ou TI.	Os usuários **se registram** e geram seus próprios dados específicos de usuário.
Autenticação em serviços internos **de diretório.**	Autenticação em **serviços públicos**, como OpenID e redes sociais, serviços de diretório e serviços externos de verificação de credenciais.
Os usuários são conhecidos e cativos: funcionários, contratados, parceiros. **A identidade pode ser assumida.**	Os usuários são **desconhecidos** (até o registro) e podem criar várias contas, algumas falsas. **A identidade não pode ser assumida.**
Os usuários da força de trabalho são **mais tolerantes** à latência e desempenho ruim porque muitas vezes **não têm alternativa.**	Clientes e clientes em potencial têm **tolerância muito baixa** por desempenho ruim e têm **muitas alternativas atraentes.**
Dimensionável de **dezenas a centenas usuários,** uma identidade cada.	Dimensionável até **centenas de milhões de usuários** com até bilhões de identidades de consumidores.
O provedor de identidade (IdP) tradicional é geralmente **um sistema central interno de TI.**	**Muitos provedores de identidade descentralizados:** login social pelo Facebook, Google, LinkedIn etc. e login tradicional.
Muitos sistemas de TI heterogêneos, em uma **rede corporativa fechada.**	Muitos sistemas de TI heterogêneos, **em redes públicas (Internet).**
Dados do perfil do funcionário coletados para **fins administrativos e operacionais.**	Dados do perfil do cliente coletados para **propósitos comerciais altamente críticos** (transações, marketing, personalização, análise e Business Intelligence).
Integração com **sistemas de RH e ERP.**	Integração com um **cenário amplo** de **tecnologia de automação de marketing** e vendas, **sistemas analíticos** e **soluções de segurança e** conformidade.
O gerenciamento de dados pessoais e a privacidade/ preferência/consentimento do usuário acontecem **em um ambiente corporativo controlado e homogêneo.**	A manipulação de dados pessoais sujeitos a uma **ampla variedade de regulamentos de privacidade e proteção de dados** que exigem que os usuários visualizem, modifiquem e revoguem as configurações de preferência e consentimento.

Leia "Desenvolver vs. comprar? Um guia para Gerenciamento de identidade e acesso do cliente" para saber mais sobre soluções de CIAM, ou visite akamai.com/identitycloud para saber mais sobre como o CIAM da Akamai permite que você forneça experiências digitais confiáveis para seus usuários finais.

FONTE

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