WHITE PAPER

Garantia de segurança da identidade digital:

Como preservar a segurança dos dados do cliente

Akamai

Resumo executivo

O gerenciamento da identidade digital e dos perfis dos clientes é fundamental para a transformação digital de todas as empresas. As identidades dos clientes e os dados pessoais associados a eles estão entre os ativos mais importantes e valiosos de qualquer organização. A proteção dessas identidades digitais, desde o registro até os estágios posteriores do relacionamento com o cliente, e a garantia de preservação do valor comercial dos dados associados são fundamentais para o sucesso dos negócios.

Ao gerenciar as identidades digitais e conquistar a confiança do consumidor, as empresas precisam aplicar as mais rigorosas medidas de segurança para proteger os clientes e a si mesmas. Na pior das hipóteses, os clientes podem se tornar vítimas de roubo de identidade, com possível impacto significativo sobre a segurança financeira, profissional e pessoal deles. Todos esses fatores podem causar não apenas a perda de confiança, mas também cobranças de responsabilidade e ações coletivas contra a empresa.

Além disso, as empresas precisam implementar rigorosas medidas de proteção da privacidade da identidade em conformidade com os regulamentos internacionais de privacidade, incluindo o GDPR (General Data Protection Regulation)[1] da União Europeia, a CCPA (California Consumer Privacy Act),[2] o PIPEDA (Personal Information Protection and Electronic Documents Act)[3] do Canadá e outros regulamentos específicos do setor, como as leis de privacidade que tratam da segurança das informações médicas.

Este artigo discute:

- *A necessidade de proteger a identidade dos consumidores por meio do CIAM (customer identity and access management) e uma infraestrutura segura e robusta*
- *A necessidade de uma funcionalidade de segurança avançada e flexível, como o acesso com escopo*
- *A importância da proteção da rede de borda*
- *Os crescentes regulamentos internacionais de privacidade*
- *Como conquistar a confiança do consumidor*
- *As vantagens do CIAM baseado em nuvem*

O artigo termina com um breve exemplo real de uma importante empresa farmacêutica que implantou uma solução CIAM segura e de melhor qualidade para capacitar seus profissionais de saúde para os regulamentos de privacidade de dados.

Proteção das identidades dos clientes

As identidades digitais dos clientes são bens valiosas. Cada vez mais, as empresas usam dados de identidade para personalizar as experiências do cliente com base em preferências, comportamento e informações demográficas. Embora tenha beneficiado tanto as empresas quanto os consumidores, a coleta de dados de identidade para personalizar experiências também aumentou o risco de violações de dados de alto custo e prejudiciais à marca.

O relatório de custo da violação de dados de 2019, realizado pela IBM Security e pelo Ponemon Institute, constatou que 48% das organizações representadas identificaram a causa raiz de uma violação de dados como um ataque mal-intencionado ou criminoso, com um custo médio de aproximadamente US$ 157 por registro de identidade violado.[4] Como as violações de segurança das informações pessoais geralmente envolvem centenas de milhares (ou até milhões) de registros de clientes, o custo resultante pode prejudicar gravemente uma empresa. E isso ocorre antes da possível perda de receita associada a danos à reputação e à perda de confiança do cliente.

A obtenção e o armazenamento de dados dos clientes, ou seja, a retenção e o processamento das credenciais e informações pessoais dos clientes, exigem extremo cuidado para evitar violação ou comprometimento de empresas e organizações. Para reforçar essa exigência, os governos criaram leis para proteger as informações de identificação pessoal (PII) dos clientes. O GDPR da União Europeia, a CCPA da Califórnia e o PIPEDA do Canadá são apenas alguns dos vários regulamentos de privacidade de dados que estão sendo promulgados globalmente.

Para que uma marca global adote as nuances dos diferentes regulamentos regionais que tratam da privacidade de dados, é preciso implementar uma estratégia que colete, processe e armazene detalhadamente as PIIs de acordo com a lei apropriada ou optar por revisar a estratégia de privacidade de dados para adequá-la à conformidade global.

Além de proteger as identidades de cada cliente, a própria infraestrutura de TI precisa ser protegida contra ameaças, como ataques DDoS (distributed denial-of-service) que poderiam, de alguma forma, resultar em tempo de inatividade, diminuição do desempenho, perda de confiança do consumidor e possíveis prejuízos financeiros. A coleta de determinados dados dos clientes pode, na verdade, ajudar a proteger a infraestrutura. Por exemplo, o endereço IP usado por um cliente pode ser registrado e verificado em uma lista negra para evitar atividades fraudulentas. Vários regulamentos mais recentes de privacidade, como o GDPR, consideram os endereços IP como informações pessoais, mas permitem a coleta e o processamento desses dados, desde que isso ocorra apenas para fins de segurança.

Proteção dos dados dos clientes

Para proteger os dados dos clientes e manter a confiança do consumidor, as empresas devem começar pela melhor solução CIAM para proteger os dados e as credenciais dos usuários por meio de rigorosa criptografia e controle de acesso com escopo. Seja com a criação de uma solução CIAM interna ou com a implantação de uma solução comercial de nível profissional, as organizações devem garantir que a solução de gerenciamento de identidades seja capaz de:

- *Proteger os dados dos clientes com rigorosa criptografia de dados em trânsito e em repouso.*

- *Fornecer controle de acesso com escopo para dados e aplicações; o controle de acesso deve ser possível até o nível dos campos de registro de dados individuais (ao contrário dos sistemas que permitem apenas "tudo ou nada") e por função e/ou atributo.*
- *Proteger as contas dos clientes contra abuso com base em métodos rigorosos de autenticação dos usuários, como autenticação de senha por etapas e de uso único (OTP) e suporte CAPTCHA de desafio-resposta.*
- *Interromper o tráfego de ataques antes que eles atinjam aplicações essenciais e causem interrupções, prejudiquem o desempenho ou aumentem os custos de computação.*
- *Atender aos requisitos das certificações e dos atestados de proteção da segurança, como a ISO (Organização Internacional para Padronização) 27001:2013 e 27018:2014, o SOC (Service Organization Control) 2 Tipo II e a CSA (Cloud Security Alliance) STAR Nível 2*
- *Permitir conformidade total com diferentes regulamentos regionais de privacidade de dados, como GDPR, CCPA, PIPEDA e vários outros regulamentos específicos do setor e da área de saúde*

Controle de acesso com escopo

Para proteger as informações de identidade do cliente, as soluções CIAM devem fornecer níveis de permissão altamente granulares para garantir controle total dos indivíduos e aplicações com direito de acesso e manipulação das informações, tudo com base em funções e responsabilidades.

O controle de acesso refinado deve ser aplicado até as colunas de dados, as linhas e os campos. Por exemplo, deve ser possível definir funções que permitam que os desenvolvedores executem tarefas de administração de aplicações sem permitir que eles obtenham acesso a qualquer dado dos clientes.

Além disso, a solução CIAM deve oferecer um conjunto de funções predefinidas com base em obrigações administrativas típicas de acordo com o princípio do menor privilégio, por exemplo, funções específicas para representantes de atendimento ao cliente que precisam acessar dados dos clientes sem permissões administrativas adicionais.

O acesso com escopo deve ser disponibilizado para funcionários e prestadores de serviço da empresa, bem como para as aplicações de vendas e marketing da organização. Este recurso pode ser muito útil para evitar a disseminação de dados tóxicos. Por exemplo, se o usuário optar por não receber comunicação por e-mail, uma solução CIAM com acesso com escopo poderá bloquear automaticamente os sistemas de automação de marketing e outras instalações impedindo que eles acessem os endereços de e-mail desse usuário.

Proteção na borda

Um componente importante da segurança da identidade digital é a proteção da rede de borda. As soluções CIAM de classe empresarial devem proteger os pontos de extremidade de registro contra ameaças cada vez mais complexas e sofisticadas, desde tentativas de violação oportunistas e sofisticadas até ataques DDoS e chamadas mal-intencionadas a APIs (application programming interface).

Quando se têm camadas que protegem os pontos de extremidade de identidades na borda da rede, é possível detectar e impedir atividades e agentes mal-intencionados antes que eles (e o tráfego de ataque potencialmente maciço que eles causam) consigam atingir os websites e as aplicações reais.

Para aumentar o desempenho das experiências de identidade, as soluções empresariais devem também aplicar a tecnologia de armazenamento em cache inteligente para garantir que os dados e as experiências dos usuários sejam mantidos próximos do usuário final.

Confiança e regulamentos de privacidade

Estreitamente associado ao conceito de segurança de identidades digitais está o conceito de garantia da privacidade do consumidor. Conforme discutido no white paper complementar "GDPR, CCPA e outros regulamentos: Como o controle de identidade ajuda as empresas a garantir conformidade regulamentar e melhorar a confiança do cliente", os crescentes regulamentos de privacidade, como o GDPR e a CCPA, estão sendo aplicados globalmente em ritmo acelerado, diante das violações de dados bastante divulgadas, roubos de ID e escândalos relacionados.[5] Somente nos EUA, dez estados apresentaram ou aprovaram projetos de lei que impõem obrigações mais abrangentes a empresas e fornecer aos consumidores mais transparência e melhor controle sobre as PIIs.[6]

As empresas não podem ignorar essas novas leis e regulamentos de privacidade. Apenas do ponto de vista financeiro, as multas moderadas que foram impostas nos primeiros 12 meses do GDPR deram lugar a multas muito maiores. A recente multa de US$ 123 milhões contra uma empresa de hotelaria internacional, em decorrência da invasão de informações pessoais de 380 milhões de hóspedes do hotel, é um exemplo importante.[7] Essas multas deverão aumentar de tamanho, até o surpreendente limite estatutário do GDPR de 4% do faturamento global anual.

Mas o custo para as empresas internacionais é muito mais do que apenas financeiro. A confiança do consumidor está em risco. As empresas atualmente precisam de consentimento explícito para processar dados pessoais. E qualquer consentimento requer confiança. Sem confiança, não há consentimento. Sem consentimento, não há dados. Tudo isso resulta em campanhas de vendas ou de marketing ineficientes.

Honrar a segurança e a privacidade não é apenas uma questão de conformidade, mas também uma vantagem comercial essencial. A segurança, a privacidade e o controle da identidade ajudam as empresas a construírem relacionamentos profundos com usuários e clientes, o que gera maior fidelidade e possível aumento da receita da empresa.

O requisito da solução CIAM moderna

De acordo com o GDPR e outras legislações de privacidade, as organizações que processam dados pessoais devem proteger os dados contra acesso não autorizado. De acordo com o GDPR, é essencial ser capaz de demonstrar que medidas de segurança "apropriadas" e "de alta tecnologia" estão protegendo os dados efetivamente.

Mas, o que é uma "medida de segurança apropriada" e qual evidência necessária é esperada? De acordo com o GDPR, as medidas de segurança apropriadas são aquelas que consideram o que há de mais avançado, o custo de implementação e o escopo, o contexto e a finalidade do processamento,

equilibrando esses aspectos com os riscos e os impactos nos direitos e nas liberdades dos indivíduos. Portanto, cabe à organização determinar o que é "apropriado" ou "equilibrado" e, consequentemente, ter como base as melhores práticas do setor.

Uma ferramenta para determinar o equilíbrio certo é a DPIA (avaliação do impacto de proteção de dados),[8] um processo exigido pelo GDPR, em alguns casos, para determinar o possível impacto das operações de processamento de dados. Quando realizar uma DPIA, uma organização deve documentar detalhadamente uma série de fatores, incluindo:

- *Operações de processamento de dados previstas*
- *Necessidade e proporcionalidade dessas operações*
- *Avaliação dos riscos de violação de dados associados às operações*
- *Medidas previstas para lidar com esses riscos, incluindo proteções e medidas de segurança, além de mecanismos para assegurar a proteção de dados pessoais*

O GDPR e outros regulamentos exigem uma abordagem com base em riscos para a proteção de dados. As obrigações de segurança dos dados não são definidas de maneira absoluta, mas devem ser desenvolvidas com base em uma ampla análise e na compreensão dos riscos que cada operação de processamento possa ter para os indivíduos cujos dados estão sendo processados.

Embora essa abordagem ofereça a flexibilidade necessária para que as organizações apliquem medidas razoáveis em função de custos, arquitetura do sistema e fatores relacionados, ela exige, no entanto, uma revisão rigorosa de custo-benefício/risco em relação a tudo o que a organização faz com dados pessoais.

O sucesso no fornecimento de provas suficientes da eficácia da atenuação de riscos de uma organização dependerá da compreensão dos riscos de privacidade relevantes, bem como dos pontos fortes das medidas mais avançadas de segurança e gerenciamento de dados a serem implementadas de acordo com a percepção dos riscos.

As vantagens da nuvem

Ao implementar os conceitos, processos e tecnologias de segurança da identidade digital discutidos neste artigo, as empresas têm duas opções básicas: desenvolver internamente ou comprar uma solução empresarial de um fornecedor especializado em CIAM.

Conforme analisado extensivamente no white paper "Build vs. Buy: A Guide for Customer Identity and Access Management" (Desenvolver ou comprar: guia para o controle de acesso e identidade do cliente), as soluções comerciais prontas, baseadas em nuvem, são geralmente a melhor opção para os objetivos, necessidades e recursos da maioria das empresas.[9] É o que acontece, particularmente, quando não apenas a implementação inicial está sendo considerada, mas também o nível de esforço necessário para operar e manter uma solução no longo prazo, com requisitos que mudam

Desde pesquisas e desenvolvimento contínuos a SLAs garantidos, as soluções de CIAM comerciais têm várias vantagens significativas em relação aos departamentos internos de TI. As soluções de nuvem adicionam escalonamento elástico, failover de várias regiões e recuperação de desastres, além dos níveis de segurança que as equipes internas dificilmente conseguiriam obter.

constantemente ditados pela tecnologia e pelos consumidores, mercados e reguladores. Em particular, as cláusulas atuais das legislações regulamentares, como o GDPR, são mais bem atendidas por soluções de terceiros, de nível profissional.

As soluções CIAM comerciais têm várias vantagens significativas em relação aos departamentos internos de TI que tentam criar uma solução própria. Desde a disponibilidade e escala globais até os SLAs (Acordos de Nível de Serviço) garantidos e certificações de segurança, as soluções CIAM comerciais têm a competência, os recursos, as pesquisas e o desenvolvimento contínuos que vêm com os fornecedores terceirizados, o que significa que as equipes de TI internas podem concentrar esforços em outras iniciativas de negócios importantes.

As soluções CIAM projetadas para utilizar os recursos de uma nuvem moderna para compartilhar recursos, fornecer escala elástica, garantir proteção e permitir failover de várias regiões e recuperação de desastres oferecem recursos de IDaaS (identidade como serviço) com uma variedade de recursos e em níveis de segurança que são frequentemente difíceis de obter com desenvolvimentos internos. Ao mesmo tempo, elas eliminam a necessidade de possuir e operar hardware e instalações de data center.

Embora o gerenciamento de identidades feito pela própria pessoa possa parecer factível, existe um risco substancial de subestimar o esforço, o subfinanciamento e a falta de recursos internos e expertise de longo prazo para apoiar, manter e evoluir a solução a fim de atender às mudanças nas exigências do mercado e às expectativas do consumidor.

Os fornecedores de CIAM comerciais estão em melhor posição para acompanhar as mudanças ditadas pela tecnologia, consumidores, mercados e reguladores, simplesmente porque os fornecedores de soluções precisam evoluir seus serviços para manter as ofertas competitivas, relevantes e em conformidade. À medida que desenvolvem suas soluções, não apenas para um, mas para muitos clientes, eles podem obter benefícios de economia de escala que simplesmente não estão disponíveis no desenvolvimento de soluções internas.

Empresa farmacêutica internacional implanta solução de gerenciamento seguro de identidades para capacitar profissionais de saúde

O desafio

Uma importante empresa farmacêutica internacional colabora com profissionais de saúde (HCPs), governos e comunidades locais para proporcionar e expandir o acesso a serviços de saúde confiáveis e econômicos em todo o mundo. No entanto, vários regulamentos de conformidade em torno da promoção de produtos e serviços para HCPs afetaram os objetivos da empresa de lançar terapias rapidamente no mercado. A empresa precisava de uma solução de controle de identidade que desse aos HCPs acesso contínuo e seguro ao seu website profissional para aproveitar as promoções de medicamentos controlados e, ao mesmo tempo, manter-se em conformidade com as regulamentações específicas do país. Para atender a essas necessidades, a empresa precisava de uma solução CIAM moderna e de nível empresarial.

A solução

A empresa selecionou o Akamai Identity Cloud para oferecer um método seguro de registro de contas, que representasse sua marca, para seu website profissional que incluísse fluxos de trabalho de login, login único, autenticação, gerenciamento de senhas, fluxos de criação de contas, validação de campos e muito mais. Os recursos de gerenciamento de perfis facilitam a edição de informações de perfil, enquanto o armazenamento de dados de perfil coleta e armazena automaticamente os dados do HCP em um banco de dados seguro, flexível e unificado na nuvem.

A plataforma Identity Cloud é nove vezes mais rápida do que a solução anterior da empresa. Ela concede aos HCPs, em todo o mundo, acesso seguro a recursos médicos regulamentados, atendendo a diversos padrões de proteção e conformidade entre regiões. Os HCPs podem agora obter amostras de medicamentos em questão de dias, em vez de semanas, pelo website seguro, melhorando, assim, o atendimento e a qualidade de vida dos pacientes. Os representantes da empresa agora obtêm ganhos de produtividade com menos visitas necessárias aos consultórios dos HCPs para entregar amostras de medicamentos e outros recursos.

Além disso, a integração do Identity Cloud com as plataformas de tecnologia de marketing existentes permite que a empresa farmacêutica personalize seus esforços de marketing para os HCPs em todo o mundo.

Akamai Identity Cloud

O Identity Cloud é a solução da Akamai para CIAM. A plataforma oferece tudo o que as empresas precisam para que seus clientes possam criar contas pessoais e fazer login com segurança em websites, aplicações móveis ou aplicações baseadas na IoT. O Identity Cloud oferece ferramentas que podem ser usadas para reduzir significativamente os esforços de conformidade com as leis de privacidade, além de ainda fornecer às empresas um repositório de perfis de clientes extremamente seguro e visão do cliente de 360°.

O Identity Cloud oferece recursos específicos e experiências de usuário que podem ajudar as empresas a atender aos requisitos normativos e de segurança. Os recursos de privacidade e proteção do Identity Cloud incluem registro de clientes, login, autenticação, login único, controle de acesso com escopo, gerenciamento de preferências e consentimentos e vários outros recursos necessários para coletar, gerenciar e proteger dados pessoais.

Com a implantação do Identity Cloud, as empresas e organizações podem implementar o gerenciamento de identidades de nível empresarial de forma rápida e flexível. Projetada com uma arquitetura nativa da nuvem, a solução se expande de forma inteligente com as necessidades de capacidade de aplicação para acomodar picos de tráfego e entregar capacidade de adaptação a centenas de milhões de usuários, bem como proteção, desempenho e disponibilidade para satisfazer as aplicações essenciais para os negócios. O Identity Cloud da Akamai foi projetado para ajudar as organizações a atender as regulamentações internacionais de proteção e privacidade, construir confiança na marca, gerenciar dados dos clientes e reduzir riscos, tornando os dados disponíveis com segurança em todas as regiões e aplicações.

Conclusão

Além de expandir os regulamentos de privacidade de dados, a proteção e a privacidade da identidade dos clientes são cruciais para organizações que desejam criar relacionamentos digitais sólidos e confiáveis com os clientes. Os consumidores têm expectativas cada vez maiores de que seus dados pessoais sejam mantidos em privacidade e segurança. Os muitos casos divulgados de abuso de dados, violações e roubo de identidade aumentaram bastante o nível de exigência para que as empresas sejam consideradas detentoras confiáveis de dados pessoais. Quando os clientes armazenam dados em uma organização, eles firmam um contrato de confiança. Se essa confiança for violada, será muito difícil restaurá-la.

FONTES

1) Regras de proteção de dados da União Europeia, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
2) Informações legislativas da Califórnia: AB-375 Privacy, https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375
3) The Personal Information Protection and Electronic Documents Act (PIPEDA), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
4) IBM 2019 Relatório sobre o Custo da Violação dos Dados, https://www.ibm.com/security/data-breach
5) White paper da Akamai: GDPR, CCPA e outros regulamentos: Como o controle de identidade ajuda as empresas a garantir conformidade regulamentar e melhorar a confiança do cliente, https://www.akamai.com/br/pt/multimedia/documents/white-paper/gdpr-ccpa-and-beyond-white-paper.pdf
6) Davis Wright Tremaine: "Copycat CCPA" Bills Introduced in States Across Country, https://www.dwt.com/insights/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou
7) ZDNet: Marriott Faces $123 Million GDPR Fine in the UK for Last Year's Data Breach, https://www.zdnet.com/article/marriott-faces-123-million-gdpr-fine-in-the-uk-for-last-years-data-breach/
8) Data Protection Impact Assessment (DPIA): How to Conduct a Data Protection Impact Assessment, https://gdpr.eu/data-protection-impact-assessment-template/
9) White paper da Akamai: Build vs. Buy: A Guide for Customer Identity and Access Management (Desenvolver ou comprar: Um guia de gerenciamento de identidades e acesso do cliente), https://www.akamai.com/br/pt/multimedia/documents/white-paper/build-vs-buy-a-guide-for-customer-identity-and-access-management.pdf

A Akamai protege e entrega experiências digitais para as maiores empresas do mundo. A plataforma de borda inteligente da Akamai engloba tudo, desde a empresa até a nuvem, para que os clientes e suas empresas possam ser rápidos e inteligentes e estar protegidos. As principais marcas mundiais contam com a Akamai para ajudá-las a obter vantagem competitiva por meio de soluções ágeis que ampliem o poder de suas arquiteturas compostas por várias nuvens. A Akamai mantém as decisões, aplicações e experiências mais próximas dos usuários, e os ataques e as ameaças cada vez mais distantes. O portfólio de soluções de segurança de borda, desempenho na Web e em dispositivos móveis, acesso corporativo e entrega de vídeo da Akamai conta com um excepcional atendimento ao cliente e monitoramento 24 horas por dia, durante o ano inteiro. Para saber por que as principais marcas mundiais confiam na Akamai, visite www.akamai.com, blogs.akamai.com ou @Akamai no Twitter. Encontre nossas informações de contato global em www.akamai.com/locations. Publicado em 11/19.