LIVRE BLANC

Assurer la sécurité des identités digitales :

Comment nous assurons la sécurité de vos données client

Akamai

Résumé

La gestion des identités digitales et des profils clients est au cœur de la transformation digitale de chaque entreprise. L'identité des clients et les données personnelles qui y sont associées comptent parmi les actifs les plus importants et les plus précieux de toute entreprise. La sécurisation de ces identités digitales, de l'enregistrement aux étapes ultérieures de la relation client, et la garantie d'une valeur commerciale continue à partir des données associées sont essentielles au succès commercial.

Lors de la gestion des identités digitales et de la création de la confiance chez les utilisateurs, les entreprises doivent appliquer les mesures de sécurité les plus strictes pour se protéger et protéger leurs clients. Dans le pire des cas, les clients pourraient être victimes d'une usurpation d'identité qui pourrait avoir des répercussions importantes sur leur sécurité financière, professionnelle et personnelle. Tous ces facteurs peuvent entraîner non seulement la perte de confiance, mais aussi des poursuites et des recours collectifs contre l'entreprise.

En outre, les entreprises doivent mettre en œuvre des mesures strictes de protection de l'identité afin de se conformer aux réglementations internationales en matière de confidentialité, y compris le Règlement général sur la protection des données (RGPD)[1], le California Consumer Privacy Act (CCPA)[2], la loi canadienne sur la protection des renseignements personnels et des documents électroniques (Personal Information Protection and Electronic Documents Act ou PIPEDA)[3] et d'autres réglementations spécifiques du secteur, comme les lois sur la protection des informations médicales.

Ce livre blanc aborde les sujets suivants :

- *La nécessité de protéger l'identité des utilisateurs grâce à la gestion des identités et des accès client (CIAM) et à une infrastructure robuste et sécurisée*
- *La nécessité d'avoir des fonctionnalités de sécurité avancées et flexibles, comme l'accès limité*
- *L'importance de la protection du réseau périphérique*
- *La multiplication des réglementations internationales en matière de confidentialité*
- *Comment gagner la confiance des utilisateurs*
- *Les avantages d'une solution CIAM basée sur le cloud*

Ce livre blanc présente en conclusion l'exemple concret d'une grande entreprise pharmaceutique internationale qui a déployé une solution CIAM sécurisée et évoluée afin d'aider ses prestataires de soins de santé à se conformer aux réglementations sur la confidentialité des données.

Sécuriser les identités client

Les identités digitales des clients sont des ressources précieuses. Les entreprises utilisent de plus en plus les données d'identité pour personnaliser l'expérience client en fonction des préférences, du comportement et des données démographiques. Bien que la collecte des données d'identité pour personnaliser les expériences ait été bénéfique à la fois pour les entreprises et les utilisateurs, elle a également augmenté le risque de violations de données potentiellement coûteuses et préjudiciables pour les marques.

Le rapport 2019 sur le coût des violations de données, mené par IBM Security et le Ponemon Institute, a révélé que 48 % des organisations représentées ont identifié la cause fondamentale d'une violation de données comme étant une attaque malveillante ou criminelle, avec un coût moyen d'environ 157 $ par dossier concerné[4]. Comme les atteintes à la protection des informations personnelles concernent souvent des centaines de milliers, voire des millions, de dossiers clients, le coût qui en découle peut nuire gravement à une entreprise. Et ce, avant de calculer la perte potentielle de chiffre d'affaires résultant d'une atteinte à la réputation et d'une perte de confiance des clients.

Collecter et stocker les données des clients, c'est-à-dire conserver et traiter les informations d'identification et les informations personnelles des clients, est un devoir de diligence que les entreprises et les organisations ne peuvent se permettre d'enfreindre ou de compromettre. En outre, les gouvernements ont adopté une loi visant à protéger les informations à caractère personnel des clients. Le RGPD de l'Union européenne, le CCPA de la Californie et le PIPEDA du Canada ne sont que quelques-uns des nombreux règlements sur la protection des données qui sont adoptés à l'échelle mondiale.

Pour qu'une marque mondiale se conforme aux nuances des différentes réglementations nationales ou régionales en matière de confidentialité des données, elle doit mettre en œuvre une stratégie qui recueille, traite et stocke les informations à caractère personnel de manière granulaire conformément à la législation en vigueur, ou choisir de réviser sa stratégie de confidentialité des données pour la rendre conforme au niveau mondial.

Au-delà de la protection de l'identité de chaque client, l'infrastructure informatique sous-jacente elle-même doit être protégée contre les menaces, comme les attaques par déni de service distribué (DDoS) qui pourraient entraîner des temps d'arrêt, une dégradation des performances, une perte de confiance des utilisateurs et des pertes financières potentielles. La collecte de certaines données clients peut aider à sécuriser l'infrastructure. Par exemple, l'adresse IP utilisée par un client peut être enregistrée et comparée à une liste noire afin d'empêcher toute activité frauduleuse. Bon nombre des nouvelles réglementations en matière de confidentialité, comme le RGPD, considèrent les adresses IP comme des informations personnelles, mais permettent de collecter et de traiter ces données tant qu'elles ne sont utilisées qu'à des fins de sécurité.

Protection des données clients

Pour protéger les données clients et préserver la confiance des utilisateurs, les entreprises devraient commencer par une solution CIAM de pointe pour sécuriser les données et les informations d'identification des utilisateurs, avec un chiffrement renforcé et un contrôle d'accès au périmètre bien défini. Qu'il s'agisse de créer une solution CIAM en interne ou de déployer une solution commerciale de qualité professionnelle, les entreprises doivent s'assurer que leur solution de gestion des identités est capable de :

- *Sécuriser les données des clients grâce à un chiffrement renforcé des données en transit et au repos*

- *Fournir un contrôle d'accès au périmètre pour les données et les applications ; le contrôle d'accès doit être possible jusqu'au niveau des champs d'enregistrement de données individuels (par opposition aux systèmes qui se limitent aux options « tout ou rien ») et par rôle et/ou attribut*
- *Protéger les comptes clients contre les abus grâce à des méthodes d'authentification utilisateur efficaces, comme l'authentification par mot de passe à usage unique (OTP) et la prise en charge des questions CAPTCHA*
- *Arrêter le trafic frauduleux avant qu'il ne puisse atteindre les applications essentielles et provoquer des pannes, dégrader les performances ou augmenter les coûts informatiques*
- *Respecter les certifications et attestations en matière de protection de la sécurité, comme l'Organisation internationale de normalisation (ISO) 27001:2013 et 27018:2014, la norme de sécurité SOC (Service Organization Control) 2 Type II et la Cloud Security Alliance (CSA) STAR Level 2*
- *Assurer la conformité totale avec les différentes réglementations régionales en matière de confidentialité des données, notamment le RGPD, le CCPA, le PIPEDA et de nombreuses autres réglementations spécifiques au secteur et aux soins de santé*

Contrôle d'accès au périmètre

Pour protéger les informations d'identification des clients, les solutions CIAM doivent fournir des niveaux d'autorisation extrêmement granulaires afin de garantir un contrôle total des personnes et des applications qui peuvent accéder aux informations et les manipuler, le tout en fonction des rôles et des responsabilités.

Un contrôle d'accès granulaire doit être appliqué jusqu'au niveau des colonnes, des lignes et des champs de données. Par exemple, il devrait être possible de définir des rôles qui permettent aux développeurs d'effectuer des tâches d'administration dans les applications sans leur permettre d'accéder aux données des clients.

En outre, une solution CIAM doit proposer un ensemble de rôles prédéfinis basés sur des tâches administratives typiques qui prennent en charge le principe de privilège minimal avec, par exemple, des rôles spécifiques aux représentants du service clientèle qui ont besoin d'accéder aux données des clients sans autorisation administrative supplémentaire.

Un tel accès doit être disponible pour les employés et les sous-traitants de l'entreprise, ainsi que pour les applications de vente et de marketing de l'entreprise. Cette capacité peut être très utile pour empêcher la propagation de données toxiques. Par exemple, si un utilisateur choisit de ne plus recevoir de communications par e-mail, une solution CIAM avec accès limité peut automatiquement bloquer l'accès des systèmes d'automatisation du marketing et d'autres installations aux adresses électroniques de ces personnes.

Protection à la périphérie

La protection du réseau en périphérie est une composante importante de la sécurité des identités digitales. Les solutions CIAM pour les entreprises doivent protéger les points de terminaison d'enregistrement contre des menaces de plus en plus complexes et sophistiquées, allant des tentatives de violation opportunistes et sophistiquées aux attaques DDoS et aux appels d'interface de programmation d'applications (API) malveillantes.

Grâce à la présence de couches de protection qui protègent les points de terminaison d'identification à la périphérie du réseau, les activités malveillantes et les cybercriminels peuvent être détectés et repoussés avant que ceux-ci (et le trafic d'attaques potentiellement massif qu'ils provoquent) puissent atteindre les sites et les applications réels.

Pour améliorer les performances des expériences liées à l'identité, les solutions d'entreprise doivent également appliquer une technologie de mise en cache intelligente pour garantir que les données et les expériences utilisateur sont conservées à proximité de l'utilisateur final.

Réglementations sur la vie privée et confiance

Le concept de protection de la vie privée des utilisateurs est étroitement lié au concept de sécurité de l'identité digitale. Comme nous l'avons vu dans le livre blanc « RGPD, CCPA et au-delà : comment la gouvernance des identités aide les entreprises à se conformer et à améliorer la confiance des clients », des règlements de plus en plus nombreux sur la protection de la vie privée, comme le RGPD et le CCPA, sont adoptés rapidement dans le monde entier, sous l'effet de violations de données, d'usurpations d'identité et de scandales connexes largement médiatisés[5]. Rien qu'aux États-Unis, 10 États ont présenté ou adopté des lois imposant de lourdes obligations commerciales afin de donner aux utilisateurs davantage de transparence et un contrôle accru sur les informations à caractère personnel[6].

Les entreprises ne peuvent pas se permettre d'ignorer ces nouvelles lois et réglementations en matière de confidentialité. Rien que d'un point de vue financier, les amendes modérées qui avaient été imposées au cours des 12 premiers mois d'application du RGPD ont maintenant cédé la place à des pénalités beaucoup plus élevées. L'amende de 123 millions de dollars récemment infligée à une grande marque d'hôtels pour piratage des informations personnelles de 380 millions de clients en est un bon exemple[7]. Et ces amendes ne vont qu'augmenter, jusqu'à atteindre le terrifiant plafond légal du RGPD qui est de 4 % du chiffre d'affaires annuel global.

Mais le coût pour les multinationales est bien plus que financier. La confiance des utilisateurs est menacée. Aujourd'hui, les entreprises ont besoin d'un consentement explicite pour traiter des données personnelles. Et le consentement nécessite de la confiance. Sans confiance, il n'y a pas de consentement. Sans consentement, il n'y a pas de données. Cela se traduit par des campagnes de vente et de marketing inefficaces.

Le respect de la sécurité et de la vie privée n'est pas seulement une question de conformité, c'est aussi un avantage commercial essentiel. La sécurité, la confidentialité et la gouvernance des identités aident les entreprises à établir des relations étroites avec les utilisateurs et les clients, ce qui se traduit par une plus grande fidélité et des revenus commerciaux potentiellement plus élevés.

La nécessité d'une solution CIAM de pointe

Selon le RGPD et d'autres lois sur la protection de la vie privée, les organisations qui traitent des données personnelles doivent les protéger contre tout accès non autorisé. Dans le cadre du RGPD, il est essentiel de pouvoir démontrer que des mesures de sécurité « appropriées » et « à la pointe de la technologie » protègent efficacement les données.

Mais qu'est-ce qu'une « mesure de sécurité appropriée » et quelles sont les preuves requises ? Selon le RGPD, des mesures de sécurité appropriées sont des mesures qui tiennent compte de l'avancée technologique et du coût de mise en œuvre, ainsi que de la portée, du contexte et des objectifs du

traitement, et qui pondèrent ces facteurs en fonction des risques et des impacts sur les droits et les libertés des personnes. Une entreprise doit donc déterminer ce qui est approprié ou adapté et se référer aux meilleures pratiques du secteur.

L'analyse d'impact relative à la protection des données[8] est l'un des outils permettant de déterminer l'équilibre. Ce processus est parfois requis par le RGPD pour déterminer l'impact potentiel des opérations de traitement des données. Dans le cadre d'une analyse d'impact relative à la protection des données, l'entreprise doit détailler un certain nombre d'éléments, parmi lesquels :

- *les opérations de traitement de données envisagées ;*
- *la nécessité et la proportionnalité de ces opérations ;*
- *une évaluation des risques de violation de données associés aux opérations ;*
- *les mesures envisagées pour faire face à ces risques, y compris les précautions, mesures et mécanismes de sécurité visant à garantir la protection des données à caractère personnel*

Le RGPD et d'autres réglementations imposent une approche de la protection des données fondée sur les risques. Les obligations en matière de sécurité des données dépendent du contexte et doivent être développées selon une analyse et une compréhension approfondies des risques que chaque opération de traitement représente pour les personnes concernées.

Bien que cette approche offre aux organisations la souplesse d'appliquer des mesures raisonnables en fonction des coûts, de l'architecture système et de facteurs connexes, elle exige néanmoins une rigoureuse analyse coût-bénéfice/risque de tout ce que l'organisation fait avec les données personnelles.

Pour fournir des preuves suffisantes d'une réduction efficace des risques, les organisations doivent comprendre les risques encourus pour la confidentialité et mettre en œuvre une gestion des données et des mesures de sécurité actualisées et efficaces en réponse aux risques perçus.

Les avantages du cloud

Pour mettre en œuvre les concepts, les processus et les technologies de sécurité en matière d'identité digitale présentés dans ce document, deux choix s'offrent aux entreprises : le développement en interne ou l'achat d'une solution d'entreprise auprès d'un fournisseur spécialisé dans le CIAM.

D'après une analyse approfondie dans le livre blanc « Conception ou achat : guide de la gestion des identités et accès clients », les solutions prêtes à l'emploi, commerciales et basées sur le cloud constituent généralement un meilleur choix pour la plupart des objectifs, des besoins et des ressources des entreprises[9]. C'est particulièrement le cas pour la mise en œuvre initiale, ainsi que le niveau d'effort nécessaire pour gérer et maintenir une solution à long terme avec des exigences en constante évolution dictées par la technologie, les utilisateurs, les marchés et les régulateurs. En particulier, les clauses exigeantes imposées par la législation réglementaire comme le RGPD sont mieux respectées par des solutions de qualité professionnelle proposées par des tiers.

Qu'il s'agisse de recherche et de développement en cours ou d'accords de niveau de service garantis, les solutions commerciales CIAM présentent plusieurs avantages significatifs par rapport aux services informatiques internes. Les solutions cloud ajoutent une évolutivité flexible, un basculement multirégional et une reprise après incident, et les niveaux de sécurité des équipes internes seraient difficiles à égaler.

Les solutions commerciales CIAM présentent plusieurs avantages importants par rapport aux services informatiques internes qui tentent de créer leurs propres solutions. Que ce soit sur le plan de la disponibilité et de l'évolutivité mondiales, des accords de niveau de service garanti (SLA) ou des certifications de sécurité, les solutions CIAM commerciales disposent des compétences, des ressources et de la recherche et du développement continus des fournisseurs tiers, ce qui signifie que les équipes informatiques internes peuvent concentrer leurs efforts sur d'autres initiatives métier clés.

Les solutions CIAM conçues pour utiliser les capacités d'un cloud récent afin de partager les ressources, d'offrir une évolutivité élastique, d'assurer la sécurité et de permettre le basculement multirégional et la reprise sur sinistre offrent des fonctionnalités IDaaS (Identity-as-a-Service) avec une multitude de fonctionnalités et des niveaux de sécurité qui sont souvent difficiles à obtenir avec le développement de solutions internes. En même temps, elles éliminent le besoin de posséder et de gérer les installations et le matériel du centre de données.

Bien que la gestion des identités en interne puisse sembler faisable, il existe un risque important par rapport à la masse de travail à prévoir, au sous-financement et au manque de ressources internes et d'expertise à long terme pour soutenir, entretenir et faire évoluer la solution afin de répondre aux exigences changeantes du marché et aux attentes des utilisateurs.

Les fournisseurs de solutions commerciales CIAM sont mieux placés pour suivre les changements imposés par la technologie, les utilisateurs, les marchés et les organismes de réglementation, tout simplement parce qu'ils doivent faire évoluer leurs services pour que leurs offres restent concurrentielles, pertinentes et conformes. Au fur et à mesure qu'ils développent des solutions non pas pour un seul mais pour de nombreux clients, ils peuvent réaliser des économies d'échelle qui ne sont tout simplement pas possibles avec le développement de solutions internes.

Une multinationale pharmaceutique déploie une solution de gestion sécurisée des identités pour aider les prestataires de soins de santé

Le défi

Une entreprise pharmaceutique internationale collabore avec des professionnels de la santé, des gouvernements et des communautés locales pour accompagner et étendre l'accès à des soins de santé fiables et abordables dans le monde entier. Mais l'entreprise, qui avait pour ambition d'accélérer la commercialisation de ses traitements, s'est heurtée à certaines réglementations régissant la promotion des produits et services auprès des professionnels de la santé. L'entreprise avait besoin d'une solution de gestion des identités permettant aux professionnels de la santé d'accéder de manière fluide et sécurisée à son site Web professionnel, afin de profiter de promotions relatives aux médicaments sur ordonnance, tout en restant en conformité avec les réglementations nationales spécifiques. Pour répondre à ces besoins, il lui fallait mettre en place une solution CIAM de pointe s'adressant aux entreprises.

La solution

L'entreprise a choisi Akamai Identity Cloud, qui procure à son site Web professionnel une solution d'inscription entièrement personnalisable, comprenant notamment des flux de connexion, l'authentification unique, l'authentification de base, la gestion des mots de passe, les flux de création de compte, la validation des champs et bien d'autres fonctionnalités. Les fonctionnalités de gestion des profils facilitent la modification des informations de profil, tandis que le stockage des données de profil recueille et stocke automatiquement les données des professionnels de la santé dans une base de données cloud flexible, unifiée et sécurisée.

La plateforme Identity Cloud est neuf fois plus rapide que la solution qu'elle utilisait avant. Elle permet aux professionnels de la santé du monde entier d'accéder à des ressources médicales réglementées, tout en respectant des normes de conformité et de sécurité géographiquement diversifiées. Les professionnels de la santé peuvent obtenir en ligne, par le biais d'un site sécurisé, des échantillons de médicaments en seulement quelques jours contre plusieurs semaines auparavant, ce qui améliore les soins et la qualité de vie des patients. Les représentants de l'entreprise ont constaté des gains de productivité, notamment grâce à une réduction des déplacements dans les cabinets des professionnels de la santé pour la fourniture d'échantillons de médicaments et d'autres ressources.

En outre, les possibilités d'intégration d'Identity Cloud aux plateformes technologiques marketing existantes a permis à l'entreprise de personnaliser ses activités marketing auprès des professionnels de la santé du monde entier.

Akamai Identity Cloud

Identity Cloud est la solution CIAM d'Akamai. La plateforme offre à toutes les entreprises les outils dont elles ont besoin pour permettre à leurs clients de créer des comptes personnels et de se connecter en toute sécurité à des sites Web, des applications pour mobile ou des applications basées sur l'IoT. Identity Cloud fournit des outils qui peuvent être utilisés pour réduire considérablement les efforts de conformité en matière de confidentialité, tout en offrant aux entreprises un référentiel de profils clients hautement sécurisé et une vue à 360 degrés sur le client.

Identity Cloud offre des fonctionnalités et des expériences utilisateur spécifiques qui peuvent aider les entreprises à répondre aux exigences de réglementation et de sécurité. Les fonctionnalités de protection et de confidentialité d'Identity Cloud incluent l'enregistrement des clients, la connexion, l'authentification de base, l'authentification unique, le contrôle d'accès au périmètre, la gestion des préférences et des autorisations, ainsi que de nombreuses autres fonctionnalités nécessaires pour collecter, gérer et sécuriser les données personnelles.

En déployant Identity Cloud, les entreprises peuvent mettre en œuvre une gestion des identités de qualité professionnelle, de manière rapide et flexible. Conçue avec une architecture cloud, la solution s'adapte intelligemment à la capacité des applications afin de s'adapter aux pics de trafic et d'offrir une évolutivité à des centaines de millions d'utilisateurs, ainsi que la sécurité, la performance et la disponibilité nécessaires pour satisfaire les applications essentielles de l'entreprise. Akamai Identity Cloud est conçu pour aider les entreprises à se conformer aux réglementations internationales en matière de sécurité et de confidentialité, à renforcer la confiance dans leur marque, à gérer les données clients et à limiter les risques en rendant les données disponibles en toute sécurité dans toutes les régions et applications.

Conclusion

Au-delà de l'extension des réglementations en matière de confidentialité des données, la sécurité et la confidentialité de l'identité des clients sont cruciales pour les entreprises qui souhaitent établir des relations digitales étroites et fiables avec leurs clients. Les utilisateurs ont des exigences de plus en plus élevées quant à la confidentialité et à la sécurisation de leurs données personnelles. Les nombreux cas largement médiatisés d'abus de données, d'atteinte à la protection des données et d'usurpation d'identité ont placé la barre encore plus haut, et on exige désormais des entreprises qu'elles soient des détentrices de données personnelles dignes de confiance. Lorsque les clients stockent des données dans une entreprise, ils concluent un contrat de confiance. Si cette confiance est rompue, il est généralement très difficile de la rétablir.

SOURCES

1) Règles de l'UE en matière de protection des données, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_fr
2) Informations sur la législation californienne : Confidentialité AB-375, 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) Rapport IBM 2019 sur le coût des violations de données, https://www.ibm.com/security/data-breach
5) Livre blanc Akamai : RGPD, CCPA et au-delà : comment la gouvernance des identités aide les entreprises à se conformer et à améliorer la confiance des clients, https://www.akamai.com/fr/fr/multimedia/documents/white-paper/gdpr-ccpa-and-beyond-white-paper.pdf
6) Davis Wright Tremaine : Dépôt de projets de loi semblables au CCPA dans les États de tout le pays, https://www.dwt.com/insights/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou
7) ZDNet : Marriott se voit imposer une amende de 123 millions de dollars dans le cadre du RGPD au Royaume-Uni pour la violation de données de l'an dernier, https://www.zdnet.com/article/marriott-faces-123-million-gdpr-fine-in-the-uk-for-last-years-data-breach/
8) Évaluation de l'impact sur la protection des données (Data Protection Impact Assessment [DPIA]) : Comment mener une évaluation de l'impact sur la protection des données, https://gdpr.eu/data-protection-impact-assessment-template/
9) Livre blanc Akamai : Conception ou achat : guide de la gestion des identités et accès clients, https://www.akamai.com/fr/fr/multimedia/documents/white-paper/build-vs-buy-a-guide-for-customer-identity-and-access-management.pdf