WHITE PAPER

Garanzia di sicurezza delle identità digitali:

Come proteggere i dati dei clienti

Akamai

Analisi riassuntiva

La gestione delle identità digitali e dei profili dei clienti è fondamentale per la trasformazione digitale di ogni azienda. Le identità dei clienti e i dati personali associati sono tra le risorse aziendali più importanti e preziose. La protezione delle identità digitali, dalla registrazione alle fasi successive del rapporto con i clienti e lo sfruttamento del valore di tali dati sono cruciali per il successo aziendale.

Per gestire le identità digitali e assicurarsi la fiducia dei clienti, le aziende devono adottare le misure di sicurezza più rigorose al fine di proteggere le proprie risorse e i clienti. Nella peggiore delle ipotesi, i clienti potrebbero subire un furto di identità, con un impatto potenzialmente significativo sulla sicurezza finanziaria, professionale e personale. Tutto ciò non solo potrebbe minare la fiducia dei clienti, ma anche comportare oneri di responsabilità e azioni legali collettive contro l'azienda.

Inoltre, le aziende devono implementare rigorose misure di protezione della privacy delle identità per conformarsi alle normative internazionali sulla privacy, come il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea,[1] il California Consumer Privacy Act (CCPA),[2] il Personal Information Protection and Electronic Documents Act (PIPEDA) canadese[3] e altre normative specifiche di settore, come le leggi sulla privacy relative alla sicurezza delle informazioni mediche.

Questo white paper illustra:

- *La necessità di proteggere le identità dei clienti con la gestione degli accessi e delle identità dei clienti (CIAM) e un'infrastruttura solida e sicura*
- *L'esigenza di una funzionalità di sicurezza avanzata e flessibile, come un accesso con ambito*
- *L'importanza di una protezione di rete sull'edge*
- *Il numero crescente di normative internazionali sulla privacy*
- *Come conquistare la fiducia dei clienti*
- *I vantaggi di una CIAM basata sul cloud*

Questo white paper si conclude con un esempio reale di un'azienda farmaceutica leader mondiale che ha implementato una soluzione CIAM di prim'ordine per consentire ai suoi provider sanitari di rispettare le normative in materia di privacy dei dati.

Protezione delle identità dei clienti

Le identità digitali dei clienti sono risorse preziose. Le aziende utilizzano sempre più spesso i dati sulle identità per personalizzare le customer experience in base a preferenze, comportamenti e aspetti demografici. Se, da un lato, la raccolta dei dati sulle identità per la personalizzazione delle experience ha portato vantaggi sia alle imprese che ai consumatori, dall'altro ha anche aumentato il rischio di costose violazioni di dati, che possono danneggiare il brand.

Il Rapporto 2019 sul costo delle violazioni di dati, condotto dall'IBM Security e dal Ponemon Institute, ha rivelato che il 48% delle organizzazioni consultate ha identificato come causa principale di una violazione dei dati un attacco dannoso o criminale, con un costo medio di circa 157 dollari per ogni record di identità violato.[4] Poiché le violazioni della sicurezza delle informazioni personali spesso coinvolgono centinaia di migliaia o persino milioni di record dei clienti, il costo che ne deriva può severamente danneggiare un'azienda. Tutto questo senza nemmeno calcolare la potenziale perdita di ricavi derivante dai danni alla reputazione e dalla perdita della fiducia dei clienti.

Acquisire e archiviare i dati dei clienti, conservando e trattando le credenziali e le informazioni personali, è un obbligo di diligenza che le aziende e le organizzazioni non possono permettersi di violare o compromettere. Inoltre, come ulteriore obbligo, i governi hanno introdotto una legislazione atta a proteggere le informazioni di identificazione personale (IIP) dei clienti. Il GDPR dell'Unione europea, il CCPA della California e il PIPEDA del Canada sono solo alcune delle tante normative in materia di privacy dei dati emanate a livello globale.

Affinché un brand globale rispetti tutti i requisiti delle varie normative locali in materia di privacy dei dati, deve implementare una strategia che raccolga, tratti e archivi in modo granulare le informazioni di identificazione personale in conformità alla legge applicabile oppure aggiornare la propria strategia di privacy dei dati per garantire una conformità globale.

Oltre a proteggere le identità dei singoli clienti, la stessa infrastruttura IT sottostante deve essere protetta da minacce, come gli attacchi DDoS (Distributed Denial of Service), che potrebbero portare a downtime, a una riduzione delle performance, alla perdita della fiducia dei clienti e a potenziali perdite finanziarie. La raccolta di determinati dati dei clienti può realmente aiutare a proteggere l'infrastruttura. Ad esempio, l'indirizzo IP utilizzato da un cliente può essere memorizzato e confrontato con una blacklist, al fine di impedire attività fraudolente. Molte delle normative più recenti in materia di privacy, come il GDPR, considerano gli indirizzi IP come informazioni personali, ma ne consentono la raccolta e il trattamento esclusivamente per motivi di sicurezza.

Protezione dei dati dei clienti

Per proteggere i dati dei clienti e conservare la fiducia dei consumatori, le aziende dovrebbero partire da una soluzione CIAM di alto livello, per proteggere i dati e le credenziali dei clienti con una crittografia avanzata e un controllo degli accessi con ambito. Che scelgano di sviluppare internamente una soluzione CIAM o di implementare un prodotto commerciale di livello professionale, le organizzazioni devono accertarsi che il proprio sistema di gestione delle identità sia in grado di:

- *Proteggere i dati dei clienti con una crittografia avanzata dei dati in transito e inattivi*

- *Fornire un controllo degli accessi con ambito per dati e applicazioni; il controllo degli accessi deve essere possibile fino al livello dei singoli campi dei dati archiviati (contrariamente a quanto avviene nei sistemi che permettono "o tutto o niente") e basato su ruoli e/o attributi*
- *Proteggere gli account dei clienti contro gli abusi mediante potenti metodi di autenticazione degli utenti, come l'autenticazione incrementale e quella tramite OTP (One-Time-Password) e il supporto per la risposta ai CAPTCHA*
- *Fermare il traffico degli attacchi prima che raggiunga applicazioni critiche causando interruzioni, una riduzione delle performance o un incremento dei costi IT*
- *Rispettare le certificazioni e le attestazioni in materia di protezione della sicurezza, come l'ISO (Organizzazione internazionale di standardizzazione) 27001:2013 e 27018:2014, il Service Organization Control (SOC) 2 Tipo II e la Cloud Security Alliance (CSA Star) Livello 2*
- *Consentire una piena conformità alle varie normative locali in materia di privacy dei dati, come il GDPR, il CCPA, il PIPEDA e molte altre normative specifiche di settore e sanitarie*

Controllo degli accessi con ambito

Per proteggere le informazioni relative alle identità dei clienti, le soluzioni CIAM devono fornire livelli di autorizzazione altamente granulari, per garantire il pieno controllo su quali utenti e quali applicazioni possano accedere o meno alle informazioni e manipolarle, in base a ruoli e responsabilità.

Un controllo minuzioso degli accessi deve essere applicato a tutte le colonne, le righe e i campi di dati. Ad esempio, dovrebbe essere possibile definire i ruoli che consentono agli sviluppatori di effettuare operazioni di gestione delle applicazioni senza permettere loro di accedere ai dati dei clienti.

Una soluzione CIAM deve anche offrire una serie di ruoli predefiniti in base alle tipiche mansioni amministrative che sostengono il principio del privilegio minimo, come ruoli specifici per i rappresentanti dell'assistenza che debbano accedere ai dati dei clienti senza ulteriori autorizzazioni amministrative.

Un tale accesso con ambito dovrebbe essere disponibile per i dipendenti e collaboratori esterni di un'azienda, ma anche per le applicazioni di vendita e marketing dell'organizzazione. Questa funzionalità può essere molto utile a prevenire la diffusione di dati dannosi. Ad esempio, se l'utente sceglie di non ricevere comunicazioni tramite e-mail, una soluzione CIAM con accesso con ambito può impedire automaticamente ai sistemi di automazione del marketing e ad altre strutture di accedere agli indirizzi e-mail di tale utente.

Protezione sull'edge

Un'importante componente della sicurezza delle identità digitali è la protezione di rete sull'edge. Le soluzioni CIAM di livello enterprise devono proteggere gli endpoint di registrazione dalle minacce sempre più complesse e sofisticate che spaziano da tentativi di violazione opportunistici e sofisticati ad attacchi DDoS e chiamate API (Application Program Interface) dannose.

Con livelli di protezione posti in essere e a protezione degli endpoint delle identità lungo il perimetro della rete, le attività dannose e i malintenzionati possono essere rilevati e respinti prima di arrivare a siti e applicazioni, evitando un traffico di attacchi potenzialmente enorme.

Per migliorare le performance delle experience di identità, le soluzioni aziendali devono anche applicare una tecnologia di caching intelligente, per garantire che i dati e le user experience restino vicino all'utente finale.

Normative sulla privacy e fiducia

Strettamente associato all'idea di sicurezza delle identità digitali è il concetto di garanzia della privacy dei consumatori. Come descritto nel white paper "GDPR, CCPA e non solo: come la governance delle identità aiuta le aziende a garantire la conformità e ad aumentare la fiducia dei clienti", la promulgazione di normative sulla privacy, come il GDPR e il CCPA, è in rapido aumento in tutto il mondo, in seguito alle ben note violazioni di dati, ai furti di identità e agli scandali correlati.[5] Soltanto negli Stati Uniti, 10 stati hanno avanzato o approvato dei disegni di legge che impongono obblighi commerciali di vasta portata, per offrire ai consumatori più trasparenza e un migliore controllo sulle loro informazioni di identificazione personale.[6]

Le aziende non possono permettersi di ignorare queste nuove leggi e normative sulla privacy. Da un punto di vista puramente finanziario, le moderate multe imposte durante i primi 12 mesi dall'entrata in vigore del GDPR ora sono state sostituite da multe molto più pesanti. La recente multa di 123 milioni di dollari a una società alberghiera multinazionale per via di una violazione delle informazioni personali di 380 milioni di ospiti degli hotel, è un chiaro esempio.[7] E queste multe sono destinate ad aumentare, fino a raggiungere lo sconcertante limite legale, previsto dal GDPR, del 4% del fatturato globale annuale.

Ma il costo pagato dalle società multinazionali è molto superiore agli oneri finanziari. È a rischio la fiducia dei clienti. Le aziende oggi hanno necessità dell'esplicito consenso prima di trattare i dati personali. E il consenso richiede fiducia. Senza la fiducia non può esserci il consenso. Senza il consenso, non ci sono i dati. E i risultati sono campagne di vendita e di marketing inefficaci.

Il rispetto della sicurezza e della privacy non è soltanto una questione di conformità, ma anche un vantaggio fondamentale per il business. La sicurezza, la privacy e la governance delle identità aiutano le aziende a creare rapporti profondi con utenti e clienti, il che comporta una maggiore fiducia e, potenzialmente, ricavi aziendali superiori.

La necessità di una CIAM all'avanguardia

In conformità al GDPR e alle altre normative sulla privacy, le organizzazioni che trattano i dati personali devono garantire la protezione dei dati contro eventuali accessi non autorizzati. Poter dimostrare l'adozione di misure di sicurezza "adeguate" e "all'avanguardia" per una protezione efficace dei dati è un requisito essenziale ai sensi del GDPR.

Ma che cos'è una "misura di sicurezza adeguata" e quali sono le prove richieste? In conformità al GDPR, per adeguate misure di sicurezza si intendono quelle misure che tengono conto dello stato dell'arte, del costo di realizzazione e di fattori quali il campo di applicazione, il contesto e le finalità del

trattamento, controbilanciandoli con i rischi e l'impatto sui diritti e sulla libertà delle persone. Perciò, un'organizzazione dovrà stabilire ciò che è "adeguato" o "equilibrato" e, di conseguenza, considerare le best practice del settore come punti di riferimento.

Uno strumento per stabilire il giusto equilibrio è la valutazione dell'impatto sulla protezione dei dati (Data Protection Impact Assessment o DPIA),[8] una procedura necessaria in alcuni casi in forza del GDPR per determinare il potenziale impatto delle operazioni di trattamento dei dati. Quando si conduce una DPIA, un'organizzazione deve documentare nel dettaglio una serie di fattori, tra cui:

- *Le operazioni previste di trattamento dei dati*
- *La necessità e la proporzionalità di tali operazioni*
- *Una valutazione dei rischi di violazione dei dati associati alle operazioni*
- *Le misure previste per affrontare questi rischi, comprese le misure di sicurezza e di protezione, e i meccanismi per garantire la protezione dei dati personali*

Il GDPR e altre normative impongono un approccio alla protezione dei dati basato sul rischio. Gli obblighi di sicurezza dei dati non sono fissati in modo avulso dalla realtà, ma devono essere sviluppati basandosi su un'approfondita analisi e comprensione dei rischi che ogni operazione di trattamento può avere per i soggetti interessati.

Anche se questo approccio offre una flessibilità tale da consentire alle organizzazioni di applicare misure ragionevoli alla luce di costi, architettura di sistema e fattori correlati, esso richiede, in ogni caso, una rigorosa analisi costi-benefici/rischi riferita a tutto ciò che l'organizzazione fa con i dati personali.

La misura in cui un'organizzazione è in grado di fornire prove sufficienti in merito all'adozione di un sistema efficace di riduzione dei rischi dipenderà dalla sua comprensione dei rischi relativi alla privacy, nonché dei punti di forza delle misure "all'avanguardia" per la gestione dei dati e della sicurezza che sceglie di implementare in risposta ai rischi percepiti.

I vantaggi del cloud

Per implementare i concetti, i processi e le tecnologie di sicurezza delle identità digitali, menzionati in questo white paper, le aziende possono scegliere fondamentalmente tra due opzioni: acquistare una soluzione di livello enterprise da un fornitore specializzato in CIAM o svilupparne una internamente.

Come analizzato ampiamente nel white paper "Creare o acquistare? Una guida per la gestione delle identità e degli accessi dei clienti", le soluzioni commerciali pronte all'uso e basate su cloud sono, in genere, la scelta migliore per la maggior parte degli obiettivi, delle esigenze e delle risorse aziendali.[9] Ciò è particolarmente vero per l'implementazione iniziale e per il livello di impegno che, a lungo andare, è richiesto per adottare e gestire una soluzione, con le variazioni dei requisiti continuamente imposte dalla tecnologia, dai consumatori, dai mercati e dagli enti regolatori. In particolare, le clausole aggiornate della normativa regolamentare, ossia il GDPR, vengono rispettate al meglio da soluzioni di terze parti di livello professionale.

Dalla ricerca e sviluppo costanti a SLA garantiti, le soluzioni CIAM commerciali presentano vari vantaggi significativi rispetto a quelle sviluppate internamente dai reparti IT. Le soluzioni cloud offrono una scalabilità flessibile, un failover in più regioni, disaster recovery e livelli di sicurezza che i team interni avrebbero difficoltà a eguagliare.

Le soluzioni CIAM commerciali presentano diversi vantaggi importanti rispetto a quelle sviluppate internamente dai reparti IT delle aziende. Dalla disponibilità e scalabilità globali ai contratti sul livello di servizio (SLA) garantiti, fino alle certificazioni relative alla sicurezza, le soluzioni CIAM commerciali si basano sulle competenze, le risorse, la ricerca e lo sviluppo costanti offerti dai fornitori terzi, il che vuol dire che i reparti IT interni potranno concentrare i propri sforzi su altre iniziative aziendali importanti.

Le soluzioni CIAM progettate per utilizzare le funzionalità di un cloud moderno per la condivisione di risorse offrono una scalabilità flessibile, garantiscono la sicurezza e permettono un failover in più regioni, mentre il disaster recovery offre soluzioni Identity as a Service (IDaaS) con numerose funzionalità, a livelli di sicurezza spesso difficili da raggiungere con le soluzioni sviluppate internamente. Al contempo, eliminano la necessità di possedere e gestire data center e hardware.

Anche se una gestione delle identità fai-da-te sembrerebbe fattibile, c'è il rischio sostanziale di sottovalutare gli sforzi, avere un budget troppo basso e non disporre, a lungo andare, delle risorse interne, né delle competenze adatte a supportare, mantenere e fare evolvere la soluzione in risposta alle mutevoli esigenze di mercato e alle aspettative dei consumatori.

I fornitori di soluzioni CIAM commerciali sono maggiormente in grado di stare al passo con le modifiche dettate dalla tecnologia, dai consumatori, dai mercati e dagli enti regolatori, semplicemente perché devono continuare ad aggiornare i propri servizi, per mantenere le proprie offerte competitive, pertinenti e conformi. Poiché sviluppano soluzioni non soltanto per uno, ma per molti clienti, possono ottenere dei vantaggi, in termini di economie di scala, non immediatamente disponibili in caso di sviluppo interno delle soluzioni.

Azienda farmaceutica internazionale implementa una soluzione sicura di gestione delle identità per aiutare i provider sanitari

La sfida

Un'azienda farmaceutica leader mondiale ha collaborato con i professionisti sanitari (HCP), i governi e le comunità locali per supportare e ampliare l'accesso a un'assistenza sanitaria affidabile e conveniente in tutto il mondo. Tuttavia, numerose normative in materia di conformità per la promozione di prodotti e servizi agli HCP ostacolavano la realizzazione degli obiettivi aziendali in merito al rapido lancio sul mercato delle terapie. L'azienda necessitava di una soluzione di gestione delle identità che fornisse agli HCP un accesso sicuro e ottimale al suo sito web per professionisti in modo che potessero usufruire delle promozioni sui farmaci da prescrizione, rispettando comunque le normative specifiche del paese. Per risolvere queste esigenze, l'azienda aveva bisogno di una soluzione CIAM all'avanguardia, di livello enterprise.

La soluzione

L'azienda ha scelto Akamai Identity Cloud per offrire una registrazione completamente brandizzata e sicura dell'account per il proprio sito web per professionisti, completa di workflow degli accessi, SSO (Single Sign-On), autenticazione, gestione delle password, flussi di creazione degli account, convalida dei campi e molto altro. Le funzioni di gestione dei profili consentono di modificare facilmente le informazioni sul profilo, mentre lo storage dei dati dei profili raccoglie e memorizza automaticamente i dati degli HCP in un database sul cloud sicuro, flessibile e unificato.

La piattaforma Identity Cloud è nove volte più veloce rispetto alla soluzione precedente dell'azienda. Consente agli HCP di tutto il mondo di accedere in modo sicuro ed equo alle risorse mediche regolamentate, soddisfacendo, al contempo, gli standard di sicurezza e conformità diversi in base alla specifica area geografica. Gli HCP ora possono ottenere campioni di farmaci in pochi giorni, anziché in settimane, tramite il sito web sicuro, migliorando la cura dei pazienti e la qualità delle loro vite. I rappresentanti dell'azienda ora notano un notevole aumento della produttività con un numero inferiore di visite presso gli uffici degli HCP per consegnare campioni di farmaci e altre risorse.

Inoltre, le integrazioni di Identity Cloud con le piattaforme tecnologiche di marketing esistenti consentono all'azienda farmaceutica di personalizzare le proprie attività di marketing rivolte agli HCO di tutto il mondo.

Akamai Identity Cloud

Identity Cloud è la soluzione di Akamai per la CIAM. La piattaforma offre tutto ciò di cui le aziende hanno bisogno per consentire ai propri clienti di creare account personali e accedere in sicurezza a siti web, app mobili o applicazioni per l'IoT. Identity Cloud offre strumenti utilizzabili per ridurre in modo significativo le attività volte a garantire la conformità alle normative sulla privacy, offrendo, al contempo, alle aziende un archivio dei profili dei clienti altamente sicuro, per disporre di una panoramica a 360 gradi sui clienti.

Identity Cloud offre funzionalità e user experience specifiche, in grado di aiutare le aziende a soddisfare i requisiti di sicurezza e normativi. Le funzioni di privacy e protezione di Identity Cloud comprendono la registrazione dei clienti, l'accesso, l'autenticazione, l'accesso SSO, il controllo degli accessi con ambito, la gestione di preferenze e consensi e molte altre funzionalità necessarie per la raccolta, la gestione e la protezione dei dati personali.

Grazie a Identity Cloud, le aziende e le organizzazioni possono implementare la gestione delle identità di livello enterprise in modo rapido e flessibile. Progettata con un'architettura cloud nativa, la soluzione è in grado di scalare in modo intelligente le esigenze di capacità dell'applicazione per supportare picchi di traffico e fornire scalabilità a centinaia di milioni di utenti, nonché la sicurezza, le performance e la disponibilità adatte a soddisfare le applicazioni business-critical. Akamai Identity Cloud è progettato per aiutare le organizzazioni a rispettare le normative in materia di sicurezza e privacy, creare fiducia nel brand, gestire i dati dei clienti e mitigare i rischi, rendendo disponibili i dati in modo sicuro in tutte le regioni e applicazioni.

Conclusione

Oltre che per soddisfare le sempre più ampie normative relative alla privacy dei dati, la sicurezza dell'identità dei clienti e la privacy sono fondamentali per le organizzazioni che desiderino costruire rapporti digitali profondi e basati sulla fiducia con i propri clienti. I consumatori hanno aspettative sempre più alte rispetto alla privacy e alla sicurezza dei propri dati personali. I tanti casi pubblicizzati di abuso di dati, violazioni e furti di identità hanno notevolmente elevato lo standard relativo alle aziende considerate degne custodi dei dati personali. Quando i clienti memorizzano i dati in un'organizzazione, stipulano un contratto di fiducia. Se questa fiducia viene infranta, in genere è molto difficile ricostruirla.

FONTI

1) Norme sulla protezione dei dati dell'Unione europea, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_it
2) Informazioni legislative della California: AB-375 Privacy, https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375
3) Il 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) Il Rapporto IBM 2019 sul costo delle violazioni di dati, https://www.ibm.com/security/data-breach
5) White paper di Akamai: GDPR, CCPA e non solo: come la governance delle identità aiuta le aziende a garantire la conformità e ad aumentare la fiducia dei clienti, https://www.akamai.com/it/it/multimedia/documents/white-paper/gdpr-ccpa-and-beyond-white-paper.pdf
6) Davis Wright Tremaine: Disegni di legge che "emulano il CCPA" introdotti negli Stati del Paese, https://www.dwt.com/insights/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou
7) ZDNet: Marriott multata per 123 milioni di dollari per inadempienza al GDPR nel Regno Unito, per la violazione dei dati dello scorso anno, https://www.zdnet.com/article/marriott-faces-123-million-gdpr-fine-in-the-uk-for-last-years-data-breach/
8) Valutazione dell'impatto sulla protezione dei dati (DPIA): Come effettuare una valutazione dell'impatto sulla protezione dei dati, https://gdpr.eu/data-protection-impact-assessment-template/
9) White paper di Akamai: Creare o acquistare? Una guida per la gestione delle identità e degli accessi dei clienti, https://www.akamai.com/it/it/multimedia/documents/white-paper/build-vs-buy-a-guide-for-customer-identity-and-access-management.pdf

Akamai

Akamai garantisce experience digitali sicure per le più grandi aziende a livello mondiale. L'Akamai Intelligent Edge Platform permea ogni ambito, dalle aziende al cloud, permettendovi di lavorare con rapidità, efficacia e sicurezza. I migliori brand a livello globale si affidano ad Akamai per ottenere un vantaggio competitivo grazie a soluzioni agili in grado di estendere la potenza delle loro architetture multicloud. Più di ogni altra azienda, Akamai avvicina agli utenti app, experience e processi decisionali, tenendo lontani attacchi e minacce. Il portfolio Akamai di soluzioni per l'edge security, le web e mobile performance, l'accesso aziendale e la delivery di contenuti video è affiancato da un servizio clienti di assoluta qualità e da un monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni all'anno. Per scoprire perché i principali brand del mondo si affidano ad Akamai, visitate il sito www.akamai.com o blogs.akamai.com e seguite @Akamai su Twitter. Le informazioni di contatto internazionali sono disponibili all'indirizzo www.akamai.com/locations. Data di pubblicazione: 11/19.