CIAM e IAM a confronto: Perché il sistema IAM tradizionale non è adatto per i clienti

Comprendere le differenze tra CIAM e IAM

L'identità digitale è al centro della trasformazione digitale di ogni azienda. Il valore dei dati del profilo dei clienti collegati alle loro identità è aumentato drasticamente, e ora è un fattore di successo cruciale per molte aziende. Forma le basi per l'analisi, la comprensione e la previsione del comportamento e dei percorsi dei clienti, dal primo contatto alle decisioni di acquisto e alla fedeltà al brand a lungo termine.

Una comune convinzione errata è che la tecnologia richiesta per la gestione degli accessi e delle identità dei clienti (CIAM) sia la stessa richiesta per la tradizionale gestione degli accessi e delle identità (IAM). Le soluzioni IAM tradizionali, chiamate anche IAM per imprese, dipendenti o forza lavoro, sono sistemi IT che garantiscono che solo la forza lavoro o i partner commerciali noti di un'azienda possano accedere alla rete aziendale e alle sue risorse.

Il fatto che, in genere, il sistema IAM tradizionale sia una soluzione pienamente collaudata in sede, porta alcune aziende all'errata supposizione che "dal momento che disponiamo già di questa tecnologia, non può essere così difficile estenderla ai nostri clienti". Alla radice di questo approccio vi è una drastica sottovalutazione delle differenze tra un sistema IAM per la forza lavoro e un sistema IAM per i clienti, nonché della complessità di gestire le identità dei clienti per le proprietà digitali rivolte al pubblico di un'azienda. Un sistema CIAM presenta svariati, e molto più complessi, requisiti rispetto a un sistema IAM per la forza lavoro; di conseguenza, riutilizzare le soluzioni IAM per la forza lavoro può essere un approccio problematico.

Un sistema IAM tradizionale non è in grado di fornire informazioni sulle identità degli utenti, sulle azioni da loro intraprese e su cosa influenza il loro comportamento digitale.

Il riutilizzo del tradizionale sistema IAM per creare una soluzione CIAM non è la risposta

Un sistema IAM tradizionale è progettato per facilitare l'accesso dei dipendenti ai sistemi interni e non è in grado di fornire informazioni sulle identità degli utenti. In effetti, l'identità viene supposta e i dati avanzati (ad esempio le azioni intraprese da un utente e ciò che influenza il suo percorso e comportamento nella sfera digitale) non possono essere tracciati. Ma le aziende hanno bisogno di questo genere di informazioni per comprendere i loro clienti e competere nel mercato digitale.

Inoltre, presso molte delle più grandi organizzazioni, i sistemi IAM tradizionali potrebbero dover gestire decine o centinaia di identità dei dipendenti. Tuttavia, i brand con volumi elevati devono gestire contemporaneamente decine, se non centinaia, di *milioni* di account dei clienti. Inoltre, i consumatori moderni non si aspettano alcun problema; una soluzione di gestione delle identità si deve estendere e ampliare per soddisfare questo carico di lavoro senza nessuna latenza percettibile.

Un recente studio condotto da Akamai ha scoperto che un ritardo di due secondi nel caricamento delle pagine web aumenta le frequenze di rimbalzo del 103% e che il 53% dei visitatori di siti mobili abbandona una pagina che impiega più di tre secondi a caricarsi.[1] Pertanto, se si verifica un errore nel vostro sistema di gestione dell'identità, oppure si verificano dei rallentamenti perché il sistema non è in grado di gestire il carico, ne risentono probabilmente i vostri tassi di conversione e il vostro profitto. Ironicamente, i picchi di carico e l'aumento del traffico dei clienti sono in genere favoriti da campagne riuscite, il che significa che un sistema di gestione delle identità lento rema attivamente contro iniziative aziendali mirate e realizzate con notevoli sforzi.

Un sistema di gestione delle identità lento rema attivamente contro iniziative aziendali mirate e realizzate con notevoli sforzi.

Le piattaforme CIAM dedicate, come Akamai Identity Cloud, sono progettate per consentire alle aziende di sfruttare al massimo i dati di profilo dei clienti. Tali soluzioni consentono customer experience ottimali e senza intoppi, pertanto operazioni come l'accesso, l'autenticazione o la gestione delle preferenze non ostacolano le attività. Inoltre, le tecnologie CIAM soddisfano l'esigenza essenziale di proteggere i dati personali sulle reti pubbliche e consentono alle aziende globali di rispettare normative sulla privacy differenti e in continua evoluzione.

La seguente tabella evidenzia le differenze principali tra il sistema IAM tradizionale e il sistema CIAM, nonché le loro applicazioni.

SISTEMA IAM tradizionale	SISTEMA IAM dei clienti
Gestire **l'identità dei dipendenti** all'interno di un'organizzazione.	Gestire **l'identità dei clienti** su siti digitali, rivolti ai clienti e multicanali (web, mobile, IoT).
Gli utenti vengono **registrati dalla loro azienda** e i loro dati di profilo chiave vengono inseriti dal reparto delle risorse umane o IT.	Gli utenti **si registrano da soli** e generano i propri dati utente specifici.
Autenticazione in base a **servizi di directory interni.**	Autenticazione in base a **servizi pubblici**, come OpenID e social media, nonché servizi di directory e servizi esterni di verifica delle credenziali.
Gli utenti sono noti e bloccati: dipendenti, appaltatori, partner. **L'identità può essere presupposta.**	Gli utenti sono **sconosciuti** (fino alla registrazione) e possono creare account multipli e falsi. **L'identità non può essere presupposta.**
La forza lavoro è **più tollerante** rispetto alla latenza e alle scarse performance perché spesso **non ha alternative.**	I clienti e i potenziali clienti hanno **una tolleranza molto bassa** rispetto a performance scarse e dispongono di **molte alternative attraenti.**
Scalabile da **10 a 100.000 utenti,** ognuno con un'identità.	Scalabile fino a **100 milioni di utenti** con diversi miliardi di identità di clienti.
Il tradizionale provider di identità (IdP) è in genere **un unico sistema IT interno centralizzato.**	**Molti provider di identità decentralizzati:** accesso di tipo social media tramite Facebook, Google, LinkedIn, ecc., oltre all'accesso tradizionale.
Molti sistemi IT eterogenei su una **rete aziendale chiusa.**	Molti sistemi IT eterogenei su **reti pubbliche (Internet).**
Dati del profilo dei dipendenti raccolti per **scopi amministrativi e operativi.**	Dati del profilo dei clienti raccolti per **scopi aziendali di primaria importanza** (transazioni, marketing, personalizzazione, analisi e business intelligence).
Integrazione con i **sistemi HR e ERP.**	Integrazione con un'**ampia gamma** di **tecnologie di marketing e automazione delle vendite**, **sistemi di analisi** e soluzioni per **la sicurezza e la conformità**.
La gestione di dati personali e privacy/preferenze/consenso degli utenti avviene solo all'interno di un **ambiente aziendale omogeneo e strettamente controllato.**	La gestione dei dati personali è soggetta **a una grande varietà di normative relative a privacy e protezione dei dati** che obbligano a consentire agli utenti di visualizzare, modificare e revocare le impostazioni su preferenze e consenso.

Leggete "Creare o acquistare? Una guida alla gestione degli accessi e delle identità dei clienti" per ulteriori informazioni sulle soluzioni CIAM o visitate il sito akamai.com/identitycloud per saperne di più su come il sistema CIAM di Akamai vi consente di fornire experience digitali affidabili ai vostri utenti finali.

FONTE

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

Akamai

Grazie alla propria piattaforma di cloud delivery più estesa e affidabile al mondo, Akamai supporta i clienti nell'offerta di experience digitali migliori e più sicure da qualsiasi dispositivo, luogo e momento. La piattaforma ampiamente distribuita di Akamai garantisce protezione dalle minacce informatiche e performance di altissimo livello. Il portfolio Akamai di soluzioni per le web e mobile performance, la sicurezza sul cloud, l'accesso remoto alle applicazioni aziendali e la delivery di contenuti video è affiancato da un servizio clienti affidabile e da un monitoraggio 24/7/365. Per scoprire perché i principali istituti finanziari, i maggiori operatori di e-commerce, provider del settore Media & Entertainment ed enti governativi si affidano ad Akamai, visitate il sito https://www.akamai.com/it/it/ o https://blogs.akamai.com/it/ e seguite @Akamailtalia su Twitter. Data di pubblicazione: 04/19.