Cybersecurity nel Retail: l’evoluzione necessaria verso l’assenza di password nell’eCommerce

La storia della vendita al dettaglio online include una continua evoluzione della modalità di utilizzo da parte dei clienti. Indipendentemente dal fatto che il rivenditore sia un marchio con una storia consolidata e negozi fisici, o un marchio giovane costruito su piattaforme social e mobile, il tipo di business con una semplice user experience è diventato un must per massimizzare i ricavi dalla spesa online.

Uno dei processi messo sotto esame è stato il login. La tipica combinazione di nome utente e password è diventata una delle principali fonti di frustrazione e di perdita di affari da parte delle organizzazioni.

La scomoda verità è che, di fronte a requisiti spesso macchinosi e a frequenti problemi di accesso, molti utenti abbandonano gli account o i carrelli online in maniera sempre piú veloce.

La buona notizia è che vale anche il contrario.

Una nostra recente ricerca su oltre 20.000 consumatori ha rilevato che, a livello globale, quasi il 60% sarebbe più propenso a spendere di più se i servizi offrissero un processo di login semplice, sicuro e senza attriti.

Questo dato è coerente con tutti i settori e i tipi di industrie. Ma il problema è più sentito da chi si rivolge ai millennial e alla generazione Z: il nostro studio ha rilevato che quasi un terzo (29%) dei giovani tra i 18 e i 29 anni non

si preoccupa della propria identità digitale e vuole solo poter acquistare rapidamente. Il messaggio è chiaro: la velocità vende.

Cosa succede dopo la prima fase delle password

Sebbene un certo tipo di divergenza sia necessario e inevitabile, per stabilire la fiducia e fornire controlli di sicurezza la nostra ricerca mostra che le password hanno raggiunto un punto critico: quasi due terzi degli intervistati si sente sopraffatto dal numero di nomi utente e password che devono essere gestite.

Una sensazione negativa che inizia con la creazione delle password. Nella nostra ricerca, il 33% degli intervistati ha dichiarato di sentirsi frustrato quando deve creare una password che soddisfi determinati requisiti.

E anche se i clienti stringono i denti e si ostinano a impostare il login con nome utente e password, i problemi non fanno che peggiorare. Il 63% degli intervistati riferisce che almeno una volta al mese non riesce ad accedere a un account perché ha dimenticato il nome utente o la password, il 24% lo fa almeno una volta alla settimana e il 6% lo fa quotidianamente.

C’è poi il problema che le password non funzionano come dovrebbero contro la complessità degli attacchi moderni. Le persone, comprensibilmente, soffrono di stanchezza da password e le riutilizzano. Allo stesso tempo, gli aggressori hanno accesso a strumenti sofisticati, che rendono davvero facile compromettere anche la password più complessa che apre più account.

A questo livello strategico, le password sono incredibilmente deboli. Le vulnerabilità delle password sono alla base di oltre l’80% delle violazioni. Nel Novembre 2022, la password

più comune al mondo era ancora “123456”. Alla luce della crescente pubblicità sull’impatto di tali violazioni e debolezze, i potenziali clienti non sono più rassicurati da un servizio “protetto da password”.

L’attrito, la frustrazione e la paura non rendono l’esperienza dell’utente positiva.

E per i rivenditori questo è un aspetto critico, poiché il nostro studio dimostra che i livelli di insofferenza aumentano quando ci si iscrive a un sito di vendita al dettaglio: preoccupazioni confermate da una ricerca di Auth0 che ha dimostrato che l’83% dei consumatori ha abbandonato il carrello o il tentativo di iscrizione perché il processo di login era troppo complicato.

Se l’esperienza utente è la selezione naturale della tecnologia, le password sono ormai dei dinosauri.

Infatti, secondo la ricerca di Gartner®: “Entro il 2025, le organizzazioni che adotteranno la gestione dell’identità e dell’accesso dei clienti (CIAM) con rilevamento convergente delle frodi e autenticazione senza password saranno in grado di ridurre il churn dei clienti di oltre la metà”. Questo livello di miglioramento del business significa che sopravviveranno solo i rivenditori online che utilizzeranno degli strumenti di autenticazione senza l’utilizzo di alcuna password.

E questi numeri prendono in considerazione aspetti che le aziende prendono in esame ancora prima di altre questioni importanti come l’accessibilità. I problemi di vista o cognitive e le funzioni motorie limitate impediscono agli utenti di navigare in processi di autenticazione macchinosi che richiedono all’utente di ricordare e inserire una password lunga e complessa. In questi casi, fare business in modo efficace non è solo più inclusivo, ma anche una fonte di sostanziale vantaggio competitivo.

La selezione naturale dietro l’assenza di password

Per cercare di risolvere questi problemi, il passaggio al login senza password è incentrato sull’utilizzo di fonti di identità dei clienti esistenti e affidabili.

Gran parte del lavoro di base è già stato fatto. Negli ultimi anni, la FIDO Alliance, un’associazione industriale, ha aiutato le aziende e gli utenti ad autenticarsi con la massima sicurezza, diminuendo i gradi di difficoltá. Lo standard WebAuthn fornisce le necessarie basi tecnologiche consentendo ai marchi di autenticare gli utenti con la crittografia a chiave pubblica anziché con una password.

Dalla nostra ricerca è emerso che i protocolli basati su questo standard, come il social login e l’autenticazione a più fattori (MFA), sono ormai considerati una realtà consolidata (anche se sembra che ci sia poco supporto per l’autenticazione biometrica). Il problema, tuttavia, non è tanto quale tecnologia scegliere, ma come implementarla al meglio.

A questo proposito, il passaggio al sistema senza password può richiedere risorse di sviluppo dedicate per un periodo di tempo prolungato, oltre a scalabilità, aggiornamenti e manutenzione dopo l’implementazione iniziale.

È per questi motivi che la maggior parte delle aziende si rivolge a un partner specializzato. Tuttavia, dato che numerosi studi e ricerche dimostrano che l’assenza di password riduce l’attrito e aumenta la conversione, si tratta di un investimento necessario per un’evoluzione tecnologica verso la direzione giusta.

A cura di **Ian Lowe**, Head of Industry Solutions, EMEA di Okta

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/cybersecurity-nel-retail-levoluzione-necessaria-verso-lassenza-di-password-

nellecommerce/