Mixpanel ha annunciato di aver subito un "incidente di sicurezza", ossia una **fuga di dati** di entità ancora non esplicita. L'azienda, poco nota al grande pubblico, ma centrale nell'infrastruttura digitale, fornisce servizi di analisi all'azienda di intelligenza artificiale **OpenAI**, monitorando le interazioni degli utenti con l'interfaccia di programmazione di ChatGPT. OpenAI ha prontamente assicurato il pubblico che, pur essendo stati **sottratti alcuni dati personali**, non risultano compromesse le informazioni sensibili. Nel frattempo, la società ha comunque deciso di sospendere la collaborazione con Mixpanel.

La violazione risale all'8 novembre, tuttavia questa è stata resa pubblica solamente ieri, giovedì 27 novembre. Nella sua nota, Mixpanel afferma di essere stata vittima di una **campagna di *smishing*** — una variante del *phishing* veicolata via SMS — e di aver adottato di conseguenza delle misure correttive, tra cui il rinnovo delle proprie password e il blocco degli accessi sospetti. OpenAI, da parte sua, precisa che l'incidente ha riguardato "un numero limitato di dati analitici relativi ad alcuni utilizzi dell'API" e ribadisce che **"gli utenti di ChatGPT e degli altri prodotti non sono stati colpiti"**. Curiosamente, però, OpenAI colloca la fuga di dati al 9 novembre, un giorno dopo la data indicata da Mixpanel.

Secondo quanto dichiarato da OpenAI — l'unica delle due aziende ad aver fornito dettagli sulla natura dei dati compromessi — gli intrusi hanno avuto **accesso a nomi, indirizzi email, identificativi degli utenti e delle organizzazioni associate**, oltre ai sistemi operativi utilizzati per collegarsi agli account e all'area geografica approssimativa degli utilizzatori del servizio. Dati che, seppur non sensibili in senso stretto, possono essere sfruttati per orchestrare campagne di *phishing* mirate e altamente persuasive. A rendere la vicenda più grave, secondo quanto riscontrato da *CyberNews*, OpenAI avrebbe trasmesso a Mixpanel **informazioni non anonimizzate**, in violazione delle pratiche fondamentali di sicurezza nella gestione dei dati.

Nonostante il dichiarato impegno alla trasparenza, resta poco chiaro cosa sia accaduto all'interno di Mixpanel per provocare l'incidente informatico. Dai comunicati ufficiali si può intuire che soggetti terzi siano riusciti a ottenere l'accesso agli account di uno o più dipendenti, acquisendo di conseguenza la possibilità di consultare i dati gestiti dalla piattaforma. Se questa ricostruzione fosse corretta, il problema riguarderebbe potenzialmente **tutte le aziende che si affidano ai servizi** di Mixpanel, una lettura che viene parzialmente confermata dal fatto che anche CoinTracker, entità di tracciamento di criptoportafogli, ha dichiarato di essere stata coinvolta nella violazione.

Ciò che è certo è che OpenAI attribuisce la responsabilità a Mixpanel, la quale sostiene tra le righe che sia colpa di un fattore umano, ovvero che dipendenti o collaboratori si siano fatti ingenuamente ingannare da qualche persuasivo truffatore. L'episodio ricalca però una

tendenza sempre più diffusa, ovvero la **violazione di dati e sistemi attraverso fornitori terzi**, subappaltatori che si dimostrano più vulnerabili delle grandi aziende tech, ma a cui vengono esternalizzati servizi di ogni tipo.

Nel 2020 si è verificato il grave incidente legato al software Orion di SolarWinds, il quale ha compromesso numerose grandi aziende e diverse agenzie governative statunitensi. Nello stesso anno, in Italia, Enel e Luxottica hanno registrato compromissioni riconducibili a fornitori tecnologici esterni. Più di recente, lo scorso 23 novembre, è emerso il caso di SitusAMC, società che gestisce informazioni su mutui e prestiti per importanti istituti finanziari di Wall Street. Questo schema di responsabilità estesa consente ad aziende come OpenAI di sostenere — con difficoltà di smentita — che gli incidenti dipendano da negligenze di terze parti e non dalle fragilità dei propri sistemi. Nonostante questo, resta legittimo chiedersi se tale argomentazione regga nella realtà dei fatti: in ultima istanza è il committente che sceglie, integra e controlla i fornitori nella propria filiera, anche quando questi si dimostrano manchevoli.

Walter Ferri

Giornalista milanese, per *L'Indipendente* si occupa della stesura di articoli di analisi nel campo della tecnologia, dei diritti informatici, della privacy e dei nuovi media, indagando le implicazioni sociali ed etiche delle nuove tecnologie. È coautore e curatore del libro *Sopravvivere nell'era dell'Intelligenza Artificiale*.