I dati in un report di Forrester Consulting per conto di Experian e in uno studio Onfido

Imprese più esposte a frodi Ict

Crescono le perdite aziendali, telecomunicazioni nel mirino

Pagina a cura
DI FABRIZIO MILAZZO

Le perdite derivanti da frodi informatiche che sono aumentate nel 2023, rispetto all'anno precedente, per il 73% delle imprese a livello globale, in particolare nel settore dei servizi finanziari in cui la percentuale delle organizzazioni che ha segnalato un aggravarsi della situazione sale al 78%.

In Italia la percentuale di imprese che segnala un aumento delle frodi arriva all'80% ed è soprattutto il settore delle telecomunicazioni a soffrirne. A rilevarlo è il report di Experian "Forrester Fraud Research Report 2023" che raccoglie le opinioni di 308 responsabili della gestione delle frodi presso aziende attive nei settori dei servizi finanziari, delle telecomunicazioni e dell'e-commerce in dieci paesi.

Inoltre, secondo lo studio "Identity Fraud Report 2024" condotto da Onfido, il 61% dei responsabili aziendali in Italia è convinto che le frodi informatiche aumenteranno nell'immediato futuro.

Perdite. I risultati del report stilato da Forrester Consulting per conto di Experian, società che fornisce servizi di informazione globale, rivelano che i fattori alla base dell'impennata di attacchi fraudolenti vanno dalla persistente pressione finanziaria sui consumatori alle numerose violazioni di dati che fanno trapelare informazioni sensibili nel dark web e alla crescente diffusione presso il pubblico di strumenti di IA generativa che hanno facilitato l'esecuzione di processi fraudolenti, anche in assenza di particolari competenze tecniche.

Il volume degli attacchi è aumentato per quasi tutte le categorie. In base agli esiti dello studio, a crescere di più sono stati gli attacchi con identità sintetica, con il 64% delle aziende dei servizi finanziari e delle telecomunicazioni che hanno registrato un aumento. Seguono i furti d'identità e gli "account takeover", ossia accessi illegittimi all'account online di una vittima, con il 60% degli intervistati che segnala un aumento in entrambe le categorie.

Nel settore dell'e-commerce, le "friendly fraud", ossia dispute illegittime aperte dal consumatore stesso, sono cresciute per il 59% dei retailer, seguite da attacchi con identità sintetica nel 54% dei casi.

Le sfide legate alla prevenzione. Secondo la ricerca, l'ostacolo più rilevante che limita la capacità delle aziende di prevenire le frodi è la mancanza di strumenti per il "device fingerprinting", ossia il riconoscimento sicuro dei dispositivi degli utenti. Al secondo posto si piazza la mancanza di una verifica biometrica dell'identità. Entrambe tali funzionalità sono divenute essenziali per prevenire le frodi, infatti i dati dei dispositivi consentono uno screening continuo e passivo dei comportamenti sospetti mentre il riconoscimento facciale consente una verifica attiva dell'identità attraverso la biometrica, considerata il metodo più affidabile per verificare l'identità digitale degli utenti.

L'Ia dà una mano. Anche il machine learning (ML) giocherà un ruolo importante nella fase di prevenzione. «I risultati della nostra indagine evidenziano come il ML sia diventato essenziale per la prevenzione delle frodi, in quanto consente di analizzare grandi quantità di dati in tempo reale, migliorando l'individuazione sia dei truffatori che dei clienti legittimi» evidenzia Giulio Virnicchi, consulente globale di Experian. «Il ML fornisce anche la struttura analitica per la biometria comportamentale e il device fingerprinting che consente alle aziende di monitorare continuamente e passivamente i clienti senza impattare sull'esperienza utente: è questa la chiave per bilanciare la crescita dei ricavi con un'adeguata prevenzione delle frodi». Dalla lettura del report emerge, inoltre, che il 72% delle aziende ritiene che il futuro della prevenzione delle frodi sarà basato su soluzioni IA/ML. I principali vantaggi derivanti dall'utilizzo di soluzioni di ML sono l'aumento dei tassi di accettazione, la riduzione delle perdite dovute alle frodi, grazie a una maggiore accuratezza nella rilevazione delle stesse, e la diminuzione del volume delle revisioni manuali e dei falsi positivi. A giudizio degli analisti, tale aspetto è di fondamentale importanza, considerato che, ad esempio, il 76% delle aziende in Italia ritiene che i falsi positivi costino alla propria attività più delle perdite dovute alle frodi. La ricerca mostra, infine, che per l'82% degli intervistati il fattore più importante nella prevenzione delle frodi basata sull'IA/ML sarà l'aggiornamento continuo e automatico del modello per essere sempre al passo con l'evoluzione delle minacce.

In Italia ancora poca IA per prevenire le frodi. Il successo dell'IA trova conferma anche nello studio "Identity Fraud Report 2024" condotto da Onfido, società che opera nel campo dell'IA per la verifica e l'autenticazione dell'identità, secondo cui, a seguito dell'introduzione di ChatGPT, i leader globali stanno toccando con mano i benefici diffusi derivanti dall'implementazione delle nuove tecnologie. In base agli esiti dell'indagine, i responsabili aziendali in Italia stanno implementando le tecnologie di IA soprattutto per aumentare l'efficienza e la produttività attraverso l'automazione dei processi (56%), per aumentare la velocità del servizio (46%) e per ridurre l'errore umano o la parzialità dei processi (43%). Ma, nonostante la convinzione che l'IA generativa rappresenti una minaccia che accelera la velocità e la quantità degli attacchi di frode, solo il 24% dei responsabili aziendali italiani stanno dando priorità al suo utilizzo proprio nella prevenzione delle frodi. Invece, il 37% si concentra sull'utilizzo dell'IA come catalizzatore per ridurre i costi operativi e migliorare i servizi digitali. In tema di frodi, un importante tema che emerge dalla lettura del focus è l'effetto della disponibilità diffusa di strumenti online e il progresso delle tecnologie di intelligenza artificiale che stanno potenziando le tattiche dei truffatori. Con l'ampia adozione della biometria come mezzo di difesa, i truffatori stanno diventando, infatti, sempre più creativi nei loro modi di attaccare. I tassi medi di frode biometrica nel 2023 sono il doppio di quelli del 2022, con un incremento di 31 volte dei deepfake (tecnica utilizzata per la sintesi di immagini umane basata sull'intelligenza artificiale). Tuttavia, solo il 23% dei responsabili aziendali italiani prevede che le frodi perpetrate dall'IA generativa diventino un problema nazionale più serio.

L'importanza degli investimenti. Alla luce di questi timori, i responsabili aziendali riconoscono che l'IA può essere la migliore difesa contro sé stessa. Negli Stati Uniti, nel Regno Unito e in Italia il 38% del campione ritiene che le applicazioni di IA generativa siano utili per automatizzare la prevenzione delle frodi e fornire agli specialisti delle frodi la possibilità di affrontare casi più delicati. Inoltre, il 34% degli intervistati italiani ritiene che queste applicazioni offriranno un vantaggio competitivo.

Infine, globalmente il 24% dei rispondenti afferma che queste applicazioni renderanno più facile identificare e fermare le frodi, dato che in Italia si ferma al 20%. «Le aziende devono rendersi conto che i recenti sviluppi dell'IA generativa e degli strumenti di deep learning stanno potenziando gli strumenti in mano ai truffatori» osserva Mike Tuchen, Ceo di Onfido. «Se non agiscono subito e non danno priorità agli investimenti nell'IA per combattere le frodi, potrebbero subire perdite catastrofiche. Con il panorama delle minacce che evolve e vede i malintenzionati tentare di sfruttare le vulnerabilità attraverso foto modificate, invio di playback deepfake su schermi, immagini stampate e maschere 2D e 3D, l'IA è fondamentale per le aziende. Con così tante opportunità di attacco online da parte dei truffatori, le aziende devono sviluppare un approccio olistico e multilivello alla prevenzione delle frodi».

Fosche nubi all'orizzonte. Peraltro, al cospetto degli scenari delineati, il 61% dei responsabili aziendali in Italia è convinto che le frodi informatiche aumenteranno. Tale preoccupazione è particolarmente elevata nelle aziende fintech (74%), seguite dal settore gaming & gambling (67%). In Italia, le frodi di identità sintetiche sono la principale preoccupazione, indicata dal 44% degli intervistati. Mentre i responsabili del Regno Unito e degli Stati Uniti hanno indicato la privacy dei dati e le violazioni del consenso come la preoccupazione più urgente per la sicurezza dell'IA (rispettivamente, 56% e 64%, dato che, invece, in Italia si attesta al 43%). Nonostante l'attenzione dell'opinione pubblica sui deepfake sia alta, questa è la minaccia percepita come più bassa in tutti i Paesi: Regno Unito (33%), Stati Uniti (32%) e Italia (27%).

Il rischio frodi e l'IA

Aziende che hanno registrato un aumento delle perdite a causa di frodi informatiche nell'ultimo anno	73%
Aziende che hanno scoperto che i falsi positivi costano più delle perdite dovute a frode	70%
Aziende che si aspettano che le perdite per frode aumenteranno nei prossimi 12 mesi	50%
Aziende che considerano la biometria il modo più efficace per verificare l'identità del cliente	77%
Aziende che considerano l'intelligenza artificiale una componente indispensabile per la prevenzione delle frodi	73%
Aziende che ritengono che il futuro della prevenzione delle frodi sarà guidato da soluzioni basate su IA/ML	72%

Fonte: Ricerca di Experian "Forrester Fraud Research Report 2023" condotta da Forrester Consulting

© Riproduzione riservata