IRTOP CONSULTING

Economia&Risparmio

Sbarca in Borsa la prima azienda che integra criteri Esg nel processo di quotazione

Irtop porta la sostenibilità a Piazza Affari con Tecno, società che realizza piattaforme a sostegno della conversione verde delle aziende e si impegna all'utilizzo responsabile dei capitali raccolti, alla trasparenza nel reporting e alla buona governance

Anna Lambiase, ceo di Irtop Consulting

La sostenibilità sbarca ufficialmente a Piazza Affari: Tecno, società di Napoli attiva nelle piattaforme tecnologiche a sostegno della conversione sostenibile delle aziende, il cosiddetto «sustaintech», è, infatti, la prima IPO Sostenibile a Euronext Growth Milan, avendo assunto la qualifica di società benefit e integrato nel processo di quotazione i criteri Esg, con l'impegno di mantenerli anche nel post IPO. Buona governance, trasparenza del reporting e utilizzo dei capitali raccolti anche in chiave Esg sono alcuni degli ingredienti imprescindibili che Irtop Consulting, la società di advisory finanziaria milanese per la quotazione e operazioni di finanziamento che ha affiancato Tecno nell'IPO, ha posto come priorità nel processo di quotazione.

Le risorse raccolte da Tecno saranno utilizzate per finanziare un progetto di espansione internazionale, attraverso operazioni di M&A e partnership strategiche, con focus sui paesi attualmente presidiati (Regno Unito e Spagna): esportando l'innovativo modello di business SustainTech. L'ammontare complessivo del collocamento è stato pari a 11 milioni di euro, di cui 9,61 milioni di euro in aumento di capitale e 1,39 milioni di euro rivenienti dall'eventuale integrale esercizio dell'opzione greenshoe in aumento di capitale.

«Siamo orgogliosi di aver affiancato Tecno nel percorso che ha portato alla prima IPO sostenibile a Borsa Italiana» spiega Anna Lambiase, amministratore delegato di IRTOP Consulting. «Tecno rappresenta un caso pionieristico: ha incorporato principi di buona governance, trasparenza nel reporting e un utilizzo responsabile dei capitali raccolti, impegnandosi a mantenerli anche nel post-IPO. Questa operazione dimostra come sostenibilità e crescita possano andare di pari passo, quando guidate da una visione strategica e sostenute da partner solidi».

Con questa operazione Irtop Consulting conferma il proprio posizionamento tra i principali operatori di Euronext Growth Milan nel ruolo di advisor finanziario a servizio della strategia di crescita delle Pmi italiane eccellenti e continuerà dopo la quotazione ad affiancare Tecno nella gestione dei rapporti con gli investitori e negli adempimenti societari informativi di natura price sensitive. «La definizione di Ipo sostenibile» non è solo formale» continua Lambiase «ma si fonda sull'integrazione concreta dei principi Esg all'interno del modello di business, della struttura di governance e della strategia di utilizzo dei capitali raccolti in fase di quotazione. Una IPO sostenibile, infatti, implica che l'intero processo di raccolta e impiego dei fondi sia guidato da obiettivi di sostenibilità misurabili, con impegni espliciti a favore della transizione ecologica, della responsabilità sociale e della trasparenza nella gestione. Inoltre, Il carattere sostenibile dell'operazione è stato validato anche a livello documentale, attraverso un prospetto informativo che incorpora elementi avanzati come una governance Esg formalizzata, un'analisi basata sul principio della doppia materialità, che valuta sia l'impatto dell'azienda sull'ambiente e sulla società, sia l'effetto dei fattori Esg sul business stesso, e impegni concreti su parità di genere, diversity & inclusion».

La finta mail dell'Agenzia delle Entrate svuota il conto corrente

Ricevere una comunicazione dall'Agenzia delle Entrate può far salire l'ansia, ma l'emozione cambia radicalmente se nel messaggio si legge che, non solo, non ci sono debiti fiscali da saldare, ma che spetta addirittura un rimborso da 500 euro. Un sogno? Purtroppo sì. In realtà si tratta di una truffa ben studiata: un'operazione di phishing diffusa via email, dove i criminali informatici sfruttano loghi, nomi e grafiche ufficiali per simulare la provenienza da enti istituzionali, banche o aziende, inducendo le vittime a fornire dati riservati o a compiere azioni pericolose.

La smentita ufficiale

È stata la stessa Agenzia delle Entrate, guidata da Vincenzo Carbone, a denunciare pubblicamente il tentativo di frode, chiarendo in una nota che lo scopo degli hacker è carpire le credenziali di accesso all'home banking degli utenti. Secondo quanto spiegato, nel testo delle email fraudolente compare un link cliccabile o un QR code che reindirizza l'ignaro destinatario verso una pagina trappola. Qui viene chiesto di selezionare una banca tra otto disponibili per poter ricevere il presunto accredito: un passaggio che, se seguito, consente ai truffatori di impossessarsi delle chiavi di accesso al conto corrente, mettendo a rischio i risparmi personali.

L'intervento

in collaborazione con CONFASSOCIAZIONI Confederazione Associazioni Professionali

Come ostacolare la crescita delle minacce alla cybersicurezza

Sulla base delle analisi comparative del Centro studi di Confassociazioni, nel nostro Paese la cybersecurity è una minaccia rilevante, soprattutto a seguito della sempre maggiore diffusione dell'IA generativa, perché i criminali stanno ricorrendo a tecnologie di intelligenza artificiale per la realizzazione di truffe e email fraudolente sempre più sofisticate, con una forte crescita nell'impiego di deepfake, ossia contenuti video e audio manipolati per ingannare le vittime.

Più nel dettaglio, nel 2024 sono stati segnalati 357 incidenti cyber gravi in Italia, pari al 10,1% del totale mondiale. L'Italia costituisce lo 0,6% della popolazione mondiale e circa il 2% del Pil globale, ma riporta una quota di attacchi cibernetici simile a quella di Paesi più grandi come Germania, Regno Unito e Francia. Nel corso dell'anno, gli attacchi informatici sono aumentati del 31%, senza grande distinzione, tanto che i settori più colpiti sono praticamente tutti, a partire da quello sanitario, governativo, militare e finanziario. L'unica eccezione a questo impatto generalizzato è quello del settore dell'informazione e dei media che vedono non solo attacchi quotidiani, ma anche una fortissima vulnerabilità ad attacchi strategici che cerca di impattare tutto il settore delle news in ottica di una vera e propria guerra ibrida.

Solo nei comparti principali di attività, stiamo parlando di una ventina di attacchi gravi al giorno con:

- incrementi del 36% negli attacchi DDoS, che compromettono la disponibilità dei servizi online;
- circa 150 attacchi ransomware che hanno coinvolto aziende e strutture ospedaliere, con richieste di riscatto per il ripristino dei dati e frequenti interruzioni operative negli ospedali;
- il settore dei servizi (trasporti, energia, banche e telecomunicazioni) – che è il settore più ricco in termini economici – è stato colpito dal 58% degli attacchi totali;
- minori impatti, anche se si tratta sempre di numeri rilevanti, per il settore manifatturiero, tra cui industrie e imprese produttive;
- importanti, ma in diminuzione gli attacchi nel settore bancario e finanziario (-8%) che riflette l'impatto positivo delle normative (come DORA e NIS2) e maggiori investimenti in sicurezza, specie nelle tecnologie AI-driven.

Detto questo e nonostante i progressi, l'Italia rimane un obiettivo centrale del cybercrime a livello di persone, imprese e Pubblica amministrazione ed è totalmente indifesa rispetto alle minacce più sofisticate.

Le priorità per ridurre il divario con gli attaccanti – come è stato più volte messo in evidenza durante l'evento "Cybersecurity & AI. Orizzonti strategici e impatti verticali" – svoltosi a Roma nella Sala Capitolare del Senato, promosso dal senatore Francesco Zaffini e organizzato da Confassociazioni e Confassociazioni Digital, in collaborazione con ENIA, Ente Nazionale per l'Intelligenza Artificiale, e Retelit – sono diverse e necessarie: costruire Data Center sul nostro territorio per garantire sicurezza, continuità e difesa nazionale – in Italia ne abbiamo appena 191, contro i 464 della Germania e i 3.840 degli Stati Uniti –, rafforzare la governance del rischio cyber in ogni settore, promuovere una vera cultura (anche attraverso processi di education diffusa) della cybersecurity ovunque, incluse filiere e scuole. E lasciare che la centralità della supervisione resti umana affinché sia sempre l'uomo a controllare l'algoritmo e non il contrario.

Angelo Deiana, *presidente di Confassociazioni* e **Andrea Violetti**, *presidente di Confassociazioni Digital*