CYBERSECURITY MADE IN ITALY

Roma, 20 giugno 2023

CENTRO STUDI

TIM

Executive Summary

Il tema degli attacchi cyber è rimasto stabilmente nella "top ten" dei rischi più probabili / imminenti del World Economic Forum dal 2012 ad oggi, in particolare nella percezione dei manager d'azienda. Fortunatamente, una volta che le imprese diventano consapevoli della necessità di una difesa contro incidenti informatici, non si torna più indietro.

ACCELERAZIONE DEL MERCATO, spinto dalla crescita degli attacchi cyber

Il mercato della cybersecurity negli ultimi due anni ha registrato tassi di crescita a due cifre: secondo i dati dell'Osservatorio del Politecnico di Milano nel 2022 e nel 2021 il fatturato è cresciuto rispettivamente del 18% e del 15%. Questa accelerazione è spinta dall'aumento dell'intensità degli attacchi registrata dal Clusit. Ciononostante, il mercato italiano è ancora in ritardo rispetto agli altri grandi mercati europei e presenta grandi margini di crescita.

POLVERIZZAZIONE DEL SETTORE della cybersecurity italiano

Il mercato italiano è costituito da una miriade di piccoli fornitori di soluzioni di sicurezza informatica, nati per fornire soluzioni mirate a specifiche criticità. Secondo gli ultimi dati, nel settore operano oltre 3100 imprese, un numero che è quadruplicato negli ultimi 5 anni. Nonostante il settore della cybersecurity europeo sia generalmente più frammentato rispetto a quelli di Nord-America e Asia-Pacifico, l'Italia ha una struttura ancora più polverizzata rispetto ad altri paesi del vecchio continente. *Il Centro Studi Tim stima che in Italia ci siano 1,6 imprese di cybersecurity per miliardo di PIL, il doppio rispetto al Regno Unito (0,8 imprese per miliardo di PIL) e superiore anche a quello della Spagna (1,2 imprese per miliardo di PIL).* La metà delle imprese è concentrata in tre regioni: Lazio, Campania e Lombardia. In Trentino-Alto Adige invece le imprese cyber presentano una dimensione mediamente superiore a quella del resto d'Italia, caratteristica che rispecchia un modello con vocazione alla costruzione di ecosistemi dedicati alla cybersecurity. La concentrazione di un elevato numero di imprese cyber in una specifica area del territorio nazionale è un fenomeno che si riscontra anche in Francia (Parigi, Bretagna, Aquitania), Germania (Renania Settentrionale-Vestfalia), Spagna (Paesi Baschi) e segue l'esempio di modelli di successo quali il Cyberspark in Israele.

EVOLUZIONE DEI MODELLI DI OFFERTA I due modelli prevalenti: "one stop shop" con soluzioni proprietarie e servizi dedicati ad uno specifico segmento di clientela

Il mercato delle imprese cyber risulta oggi polarizzato tra tante piccole realtà, molto specializzate che fanno fatica a crescere, e grandi gruppi ICT il cui portafoglio di offerta include anche i servizi cyber. Tra questi due poli opposti si colloca un numero ristretto di imprese di media dimensione specializzate in cybersecurity che in alcuni casi sono riuscite a rafforzare il proprio percorso di crescita con la quotazione in Borsa. Lo studio si è focalizzato sulle realtà più dinamiche, in modo da

evidenziarne i tratti caratteristici e comuni al modello di evoluzione che ha premiato le imprese che sono riuscite a compiere l'auspicato salto dimensionale.

Dall'analisi del campione di imprese esaminato emergono due percorsi prevalenti:

1) Imprese che sono state in grado di crescere partendo da uno specifico prodotto "originale" (ad esempio, SIEM Security information and event management, oppure test di vulnerabilità) ed affiancando a tali tecnologie proprietarie e distintive sviluppate "in house" una più ampia gamma di servizi in grado di coprire a 360 gradi le esigenze delle PMI italiane. In particolare, ***secondo l'analisi del Centro Studi TIM, i 3/4 delle società cyber del campione esaminato possiede almeno un prodotto proprietario e più della metà hanno portafogli di offerta che coprono la quasi totalità dei servizi di cybersecurity***.
2) Imprese che forniscono soluzioni verticali ad una particolare tipologia di clienti operanti in ambiti ICT altamente specializzati (ad esempio fornitori di servizi cloud, fornitori di servizi IoT o clienti di uno specifico settore come banche, comparto dei servizi finanziari, ecc.).

ESTERNALIZZAZIONE della cybersecurity da parte delle PMI italiane

Le imprese italiane si collocano agli ultimi posti in Europa in termini di personale con competenze ICT. Secondo le stime realizzate dal Centro Studi TIM, ***il 60% delle imprese italiane sopra i 10 addetti ricorre interamente a personale esterno per le esigenze della cybersecurity e questa percentuale si avvicina al 70% quando prendiamo in esame le aziende sotto i 50 addetti***.

Disponendo di scarse competenze informatiche, le PMI devono affidarsi integralmente ai propri fornitori di sicurezza informatica, senza capacità autonoma di apprezzare e/o valutare la bontà e l'adeguatezza delle soluzioni che vengono loro proposte. Se i piccoli fornitori di cybersecurity non sono in grado di fornire una risposta esaustiva alle esigenze delle PMI italiane, i fornitori medio-grandi di soluzioni ICT non sono specializzati nella sicurezza informatica e tipicamente si avvalgono di soluzioni chiavi in mano di grandi player internazionali di cybersecurity oppure, acquisiscono piccole realtà cyber e poi integrano le soluzioni di queste ultime all'interno del proprio portafoglio d'offerta.

Le PMI e il modello del medico di base

Più che di un venditore specializzato nella fornitura di uno specifico servizio cyber, le PMI italiane hanno bisogno di un consulente in materia di cybersecurity. Le esigenze delle PMI non sono in realtà molto distanti da quelle che ciascuno di noi sperimenta quando ha bisogno di assistenza medica. Difficilmente, infatti, ci rivolgiamo direttamente allo specialista senza prima fissare un appuntamento con il medico di base (generalista); è poi quest'ultimo che, sulla base delle informazioni acquisite, ci indica la cura o ci indirizza verso lo specialista più adeguato.

Alle PMI serve una figura che, oltre a svolgere contemporaneamente il ruolo di medico di base e di medico specialista, sia anche in grado di fornire e somministrare le cure necessarie (farmacia e servizi ospedalieri). Si va quindi nella direzione di un ulteriore ampliamento del modello "one stop shop" già intrapreso con successo dalle società quotate in borsa.

Cybersecurity Made in Italy Challenge e la figura del broker di contenuto

A conferma della diffusa e riconosciuta importanza di poter contare su un settore di cyber security "domestico" sia l'Europa (con il progetto "Cyber security made in Europe"), sia in altri paesi membri quali Francia e Germania (rispettivamente con i progetti "Cyber Expert" e "IT Security Made in Germany") si sono promosse iniziative che puntano a stimolare e consolidare la crescita del settore anche all'interno dei rispettivi confini.

Lo scopo del "Cybersecurity Made in Italy Challenge" è quello di consolidare la crescita delle piccole realtà italiane ed europee che vantano prodotti all'avanguardia tecnologica e che, tuttavia, sono ancora tutt'oggi alla ricerca di un solido percorso di crescita organica. In altri termini, questa iniziativa ha l'obiettivo di facilitare l'incontro tra imprese "Pure Cybersecurity", che dispongono di soluzioni e competenze ultra-specialistiche, e le esigenze ed i bisogni manifestati più o meno consapevolmente dalle PMI italiane. Un anello di congiunzione tra domanda ed offerta che sia in grado di completare il panorama dell'ecosistema della cybersecurity.

La condivisione e "apertura" degli asset del Gruppo verso realtà esterne rappresenta un modello che TIM intende portare avanti in maniera sempre più continuativa e strutturata anche per alimentare lo sviluppo dei servizi che possono essere offerti attraverso le reti 5G, che offrono nuove e interessanti opportunità di crescita B2B e richiedono la costruzione di solide partnership con attori di altri settori (dalla mobilità alla manifattura, dalla salute ai servizi finanziari). Maggiore è la possibilità di creare connessioni, anche inusuali, all'interno degli ecosistemi che costituiscono il settore digitale italiano, maggiore è la possibilità di far crescere tutta la filiera e accelerare la digitalizzazione e l'innovazione del Paese.