PROFESSIONISTI DEL RISPARMIO

SOLDI IN TESTA

Lo strabismo degli italiani per il rischio

di **Marco Lo Conte**

Azioni e immobili si specchiano in questa fase come le figure in una carta da gioco: l'equity, come avete letto nella storia di copertina di questo numero di Plus24, ha discreti margini di crescita nonostante la cavalcata decennale; ma, per una moltitudine di fattori, vive una crisi di fiducia che allontana chi ha denaro da investire, tanto che la raccolta in fondi azionari è salita in modo risibile rispetto ai prodotti assicurativi, obbligazionari e bilanciati. Dall'altra parte il mercato immobiliare che registra una leggera contrazione del -1,7% delle compravendite, se si considera il dato destagionalizzato, attestandosi a un livello molto prossimo rispetto al 2010. Assolutamente comprensibile nel segmento abitativo ed economico, vista la correlazione con il ciclo economico, i consumi e la propensione all'indebitamento (mentre per quanto riguarda il settore business si parla esplicitamente di rischio bolla). Il tutto con prezzi sostanzialmente stabili e senza una direzione netta in un senso o nell'altro. Tutto ciò, in presenza di un eccesso di fiducia da parte della platea di investitori nel mattone. Uno strabismo paradossale tra il timore di investire in un mercato che mostra segni di forza e il credito spropositato per quello più rischioso e illiquido per antonomasia. Le ragioni, si sa, sono psicologiche e culturali e hanno fornito uno spunto importante per un recente occasional paper della Banca d'Italia «Avversione alle perdite nelle valutazioni dei prezzi degli alloggi tra gli italiani i proprietari di abitazione» di Andrea Lamorgese e Dario Pellegrino. Da cui emerge come la valutazione che viene assegnata al valore "corrente" di un immobile da parte del suo proprietario sia influenzata dal prezzo di acquisto; questa valutazione viene rivista verso l'alto quando i prezzi sono in crescita, ma non al ribasso in caso di potenziale perdita rispetto al valore di acquisto. Lo studio prende in esame un'ampia quantità di dati di mercato degli ultimi tre lustri, verificando questa dinamica. Questa *loss aversion*, secondo lo studio, è più marcata per le famiglie più povere e con minor livello di istruzione. Il che fa ben sperare per l'efficacia dell'impatto che piani di educazione finanziaria possano produrre.

FALLE INFORMATICHE

Banche, sulla cybersecurity occorre investire meglio

Le banche rimodulano i budget per la security antipirateria. Ma per gli esperti non sempre sono denari ben spesi

Stefano Elli

Nel comunicato del 28 ottobre 2019 UniCredit ammetteva che un virus iniettato nel 2015, aveva infettato i sistemi intercettando e incamerando dati di milioni di clienti. La banca si affrettava a rassicurare gli utenti: non si trattava di dati sensibili ma, in ogni caso, istituiva un numero verde dedicato alla segnalazione di anomalie. E informava di avere investito, dal 2016, oltre 2 miliardi di euro nell'implementazione di strutture volte alla prevenzione di aggressioni cibernetiche vantando una task force antipirateria formata da 400 specialisti. Nessuno è perfetto. L'anno precedente in Uk sette banche e non delle più piccole (Banco Santander, Royal bank of Scotland, Tesco Bank, Hsbc, Lloyds, Clydesdale and Yorkshire Banking group e Barclays) sono rimaste vittime di intrusioni. Dal 2012 al 2017, poi, si sono registrati 12 attacchi ai danni delle Banche Centrali di vari Paesi. Incluse le Federal reserve di Cleveland e di New York. L'ultimo rapporto Kroll sulle frodi alle imprese, nella sezione dedicata all'Italia, indica che i manager intervistati attribuiscono al furto di dati il 34% degli "incidenti" occorsi in azienda. Di più: indica che l'83% di loro è convinto che i data breach da parte di pirati informatici siano tra le tre priorità assolute. Ma che l'allarme sia rosso (scarlatto) ce lo dice l'ultimo dato: in testa alle preoccupazioni sui rischi dei prossimi cinque anni (il 66% degli intervistati) c'è proprio l'eventualità di cyberattacchi coordinati su vasta scala.

«E questo è ancora più vero nel sistema bancario italiano ma non solo italiano - spiega Roberto De Vita, avvocato e presidente dell'osservatorio Cybersecurity di Eurispes - è plausibile infatti che l'espansione dei nuovi sistemi di pagamento elettronici possa creare nuove e ancora inesplorate sacche di vulnerabilità nelle infrastrutture high tech. E la spiacevole sensazione è che, a fronte di investimenti quantitativamente rilevanti, non vi siano sufficienti conoscenze manageriali per valutarne la qualità. Cyber risk e visione strategica sono l'approccio corretto. Spesso invece si ritiene sufficiente un approccio meramente tecnico». Che i budget delle banche si stiano rimodulando per fare fronte a questi rischi lo si evince dalle più recenti statistiche dall'Abi (vedere grafici a fianco) 14 banche interpellate sul tema hanno quantificato al 26 % il totale degli stanziamenti su prevenzione e contrasto delle frodi sul totale destinato alla sicurezza It. Mentre la ripartizione del budget legato al contrasto delle frodi parla del 36% destinato a iniziative della banca, 38% all'adeguamento alle normative, e al 26% all'evoluzione del servizio alla clientela. Sul tipo di "nemico" da affrontare non sembra esservi alcun dubbio. Venti banche interpellate da AbiLab hanno risposto che le due principali tipologie di "aggressori" al retail sono i Crimeware (53,4% delle aggressioni) e i Phishing: 36,1%. Mentre le 11 interpellate sulla clientela corporate hanno indicato una quota di crimeware dell'86,3%. Si sta facendo tanto? Si sta facendo poco? Per Umberto Rapetto, consulente, a lungo comandante del Nucleo frodi tecnologiche della Guardia di Finanza, la risposta è scontata: «Il denaro non manca. Sembra piuttosto che da parte dei manager, non vi sia la capacità di "fare la spesa", cioè di comprendere il problema, di valutarlo e di impostarlo correttamente. Un paradosso: mettere dei nerboruti bodyguard a guardia delle infrastrutture It non serve a proteggerle. Semmai serve ai manager per proteggere le loro poltrone in caso di data breach. Ciò di cui c'è bisogno è pianificazione strategica e analisi dei rischi. Che oggi, va detto, non esiste proprio».

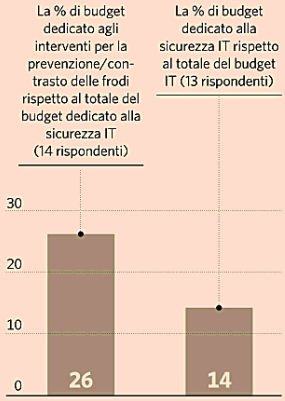
Le insidie e le contromisure

GLI STANZIAMENTI

Dati in percentuale

Ripartizione del budget destinato nel 2019 a progetti/ interventi legati al contrasto e alla prevenzione di frodi informatiche(14 rispondenti)

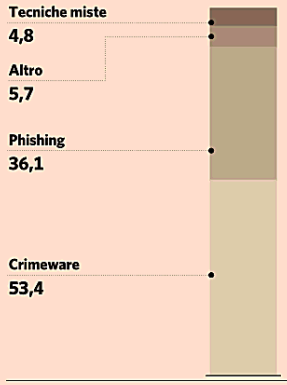
Percentuale di budget dedicato alla prevenzione/ contrasto frodi e alla sicurezza IT



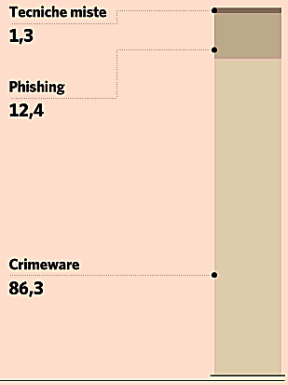
LE INSIDIE

Dati in percentuale

Vettori di attacco Clientela Retail (20 rispondenti)



Vettori di attacco Clientela Corporate (11 rispondenti)



FONTE: AbiLab, osservatorio cyber knowledge & security awareness 2019

I clienti di Afx, i soldi spariti e l'odissea tra Londra, Cipro e Roma

Risparmiatori beffati dal broker online in cerca di risposte

Una vicenda che si trascina da nove anni quella della Afx Capital, società battente bandiera cipriota, ramificazioni a Londra ma con solide radici italiane. E che vede come vittime alcune centinaia di clienti che, investendo sulle piattaforme online del broker, hanno perso decine di milioni. Le ultime tappe della vicenda le rievoca l'avvocato Donato Cecca che assiste un centinaio di loro: «Nel luglio scorso l'Authority cipriota, la Cysec, ha sospeso la licenza di Afx in attesa di chiarimenti; a inizio novembre tale licenza è stata sospesa definitivamente. Nel frattempo è intervenuta l'Authority britannica, Fca che a sua volta ha revocato la licenza e commissariato l'intermediario. In seguito , la società Cg Recovery (il Commissario incaricato), dopo avere effettuato varie ricerche nei conti riconducibili alla società ha comunicato di aver rinvenuto solo 458 mila sterline rispetto agli 8 milioni che avrebbero dovuto esserci. La Consob, dal canto suo, si è limitata a prendere atto della situazione. Al momento, i miei clienti risultano tutti legati alla società cipriota e, come stabilito dalla legge locale, hanno come salvagente 20mila euro (somma garantita agli investitori in caso di default dell'intermediario), una cifra che in quasi tutti i casi non ristora minimamente il danno subito. Se i clienti facessero riferimento alla sede di Londra potrebbero almeno contare su un ristoro parziale sino a 100mila euro». Il problema, dice Cecca, è che da luglio la Cysec non dà notizie e si sa solo che c'è in corso un'indagine.

«Diffide e richieste di rimborso non hanno sortito nessun effetto e temo che sarà necessaria qualche ulteriore azione legale». Una vicenda strana. Che sembra sparita dai radar degli inquirenti di Milano che avevano a suo tempo aperto un'inchiesta, Di cui non si sa più nulla. — **St.E.**