BANCHE Per contrastare i reati informatici bastano le legge esistenti ma vanno applicate. Gli istituti di credito italiani hanno dato il loro contributo con investimenti per 6 miliardi di euro. Parla Patuelli (Abi)

Strategia anti-hacker

di **Luca Gualtieri**

La truffa ai danni dell'ex presidente di Fideuram, Paolo Molesini, è solo l'ultimo episodio di una serie crescente di violazioni informatiche che stanno colpendo il mondo bancario e finanziario. Per Antonio Patuelli, presidente dell'Abi, la risposta non passa però soltanto da nuove norme: occorre innanzitutto applicare con rigore quelle esistenti, investire in tecnologia e formazione e ridurre l'asimmetria regolamentare tra banche e operatori digitali. Queste alcune delle osservazioni fatte martedì 22 settembre a Milano in apertura di WeSec, il Salone della Sicurezza focalizzato su sicurezza, intelligenza artificiale e infrastrutture.

Domanda. Patuelli, pochi giorni fa sono circolati video falsi del governatore della Banca d'Italia utilizzati per promuovere investimenti finanziari. Con l'Ai dobbiamo aspettarci frodi sempre più sofisticate?

Risposta. Quello che hanno fatto al governatore della Banca d'Italia lo hanno fatto a me cinque anni fa. Presentai denuncia. Erano state utilizzate mie immagini per cercare di truffare delle persone attribuendomi la responsabilità dell'iniziativa. L'indagine si arenò di fronte a difficoltà tecniche perché il sito risultava nato in Africa ed era schermato. Da allora sui siti dell'Abi e della mia banca è specificato che il presidente Patuelli non è sui social.

D. Serve quindi una nuova legislazione per affrontare questo tipo di reati?

R. No. Dobbiamo essere molto chiari: le norme italiane, a cominciare dalla Costituzione e dal codice penale, non riguardano soltanto la vita reale. Sono norme generali e astratte e devono essere applicate a ogni aspetto della società, compreso quello immateriale. Se una persona commette una truffa attraverso le nuove tecnologie deve essere perseguita come se avesse commesso una truffa con metodi tradizionali. Prima di sostenere che manca una legge, bisogna applicare quelle esistenti. Chi ha tentato di utilizzare l'immagine del governatore per una truffa deve essere perseguito fino in fondo.


Antonio Patuelli Abi

D. In questi anni si è parlato molto di educazione finanziaria dei clienti. Ma le frodi diventano talmente sofisticate da poter colpire anche gli operatori finanziari. Quanto contano la tecnologia e la preparazione del personale bancario?

R. Una delle truffe oggi più frequenti è quella del finto carabiniere. Vengono clonati perfino i numeri telefonici delle stazioni e vengono impersonate proprio le persone che godono della maggiore credibilità sul territorio. Le banche sono attrezzate innanzitutto attraverso le relazioni personali. Se allo sportello arriva una persona trafelata che vuole effettuare un bonifico istantaneo verso un soggetto sconosciuto, senza una fattura o una motivazione chiara, il dipendente può insospettirsi. Sono numerosi i casi nei quali il personale bancario riesce così a sventare una truffa.

D. Con l'home banking però questa barriera umana viene meno.

R. Esattamente. Il bonifico istantaneo può essere effettuato da casa e in quel caso non c'è il dipendente della banca che può intervenire come una sorta di angelo custode. Il rischio aumenta. Le innovazioni tecnologiche rappresentano libertà in più, ma ogni libertà porta con sé anche rischi di truffa e di condizionamento e richiede quindi maggiore responsabilità. Le banche impiegano risorse umane, denaro e tempo e lavorano quotidianamente con le forze dell'ordine. I nostri apparati di sicurezza e prevenzione sono a disposizione dell'autorità giudiziaria. Il malaffare è vecchio quanto il mondo: oggi assistiamo a una sua evoluzione tecnologica.

D. L'intelligenza artificiale può però rendere gli attacchi molto più potenti. È necessario porre limiti più stringenti alle nuove tecnologie, soprattutto quando vengono applicate a settori sensibili come finanza e risparmio?

R. Non è la prima innovazione dell'ultimo secolo ad avere un impatto enorme e una duplice potenzialità. Pensiamo all'energia nucleare: può avere impieghi pacifici oppure distruttivi. Anche l'intelligenza artificiale è un elemento di grande novità e di grande impatto e non può vivere senza regole. L'Unione europea è l'entità giuridica del mondo libero che ha realizzato le normative più mature in un quadro di democrazia e libertà. Da questo punto di vista l'Europa è più avanti perché conserva la cultura della separazione dei poteri.

D. Quanto investono le banche italiane per difendersi dalle minacce informatiche?

R. Gli investimenti complessivi in innovazione tecnologica e tutela della sicurezza superano 6 miliardi di euro. E bisogna fare attenzione: in questa cifra non rientra la formazione professionale, che compare in altre voci dei bilanci bancari, e non sono comprese tutte le spese sostenute dalle società esterne ai gruppi. Stiamo quindi sostenendo un impegno molto rilevante per la sicurezza e per la tutela del risparmio, delle imprese e delle famiglie. È un servizio di interesse generale svolto da aziende private e dovrebbe essere maggiormente riconosciuto dalle istituzioni.

D. Resta però un problema di asimmetria regolamentare: banche e operatori tecnologici possono offrire servizi simili, ma sono sottoposti a regole e controlli diversi.

R. Le istituzioni Ue e italiane mostrano una crescente sensibilità su questo tema. Da anni chiediamo che esista un terreno competitivo uguale per chi svolge lo stesso lavoro. Non può esserci una situazione nella quale alcuni operatori lavorano con una licenza e con tutti gli obblighi conseguenti mentre altri operano senza essere sottoposti allo stesso livello di regolamentazione. Dei passi avanti sono stati fatti, anche grazie all'attenzione della Bce, dell'Eba, della Bankitalia, delle autorità di garanzia e dei ministeri competenti. (riproduzione riservata)