Rubrica "Ferri del Mestiere"
Pubblicato sabato 9 luglio 2022

Truffe informatiche, come regolare i conti tra banca e clienti

I servizi di home banking per disporre operazioni di pagamento dal proprio PC rappresentano ormai un'indubbia semplificazione che ha cambiato (talvolta spersonalizzandolo) il rapporto banca/cliente.


Perito Nft cercasi

Truffe informatiche, come regolare i conti tra banca e clienti

Per garantire massimi livelli di protezione dei pagamenti online si sono succedute diverse direttive (Payment Services Directive n. 2007/64 PSD e n. 2015/2366 PSD2 recepite in Italia, rispettivamente con il d.lgs 11/10 e il d.lgs 218/17) e regolamenti Ue, volte a imporre alle banche l'adozione di presidi tecnici avanzati. Si è così passati da un sistema di autenticazione mediante il semplice inserimento di username e password a sistemi più evoluti (autenticazione forte) volti a introdurre anche le "one time password" generate volta per volta da dispositivi in possesso del cliente.

Di pari passo i pirati informatici hanno affinato i metodi per carpire le credenziali: dal malware Zeus (comparso nel 2007 e che, installato sul PC registrava, le credenziali immesse sul sito della banca) ai fenomeni di phishing (email fraudolente), nelle diverse declinazioni di smishing (sms fraudolenti), vishing (truffe telefoniche) e spoofing (che combina le due tipologie di truffe). Metodi subdoli, che consentono di modificare il mittente di un sms o di una email, riferendo apparentemente la comunicazione alla banca, provvisti di link con cui carpire credenziali e dati dell'utente. Al tutto s'accompagna la telefonata di un presunto operatore della banca (spesso previa clonazione del numero della banca) che, facendo credere di dover stornare un'operazione non autorizzata, ottiene dal cliente la one time password per disporre il pagamento.

I più avveduti (anche grazie alle campagne antiphishing delle banche) cestinano i messaggi, gli altri, allarmati dalla comunicazione, danno seguito al contatto cadendo nella trappola. Il risultato è un crescente contenzioso giudiziario nel quale viene contestata alla banca l'esecuzione di operazioni non autorizzate e l'inadempimento agli obblighi di protezione.

A chiarire quale debba essere la corretta distribuzione degli obblighi in capo al cliente e alla banca ha provveduto il Tribunale di Milano con la pronuncia 4995 del 7/06/22.

Secondo i giudici milanesi, se da un lato alla banca è imposta l'adozione di meccanismi di autenticazione forte basati su due o più elementi classificati nella categoria della conoscenza (user e password), possesso (dispositivo per generazione codice) e inerenza (utilizzo di dati biometrici), dall'altro lato, il cliente ha l'obbligo di custodire le credenziali per esprimere il consenso (art. 7 d.lgs 11/10). La prova dell'adozione di sistemi di autenticazione forte e della negligenza da parte del cliente, intesa quale indempimento agli obblighi di custodia (divulgazione dei dati a terzi), denota una colpa grave del cliente (vieppiù accresciuta da elementi di anomalia quali alert dell'operazione) e dunque l'esclusione della responsabilità della banca.

E per tali tipologie di truffe la creazione dell'alias telefonico o email non è sufficiente a provare l'hackeraggio dei sistemi bancari, dato che tale evento si verifica nella sfera giuridica delle parti della comunicazione (il cliente e il truffatore) ai quali la banca è estranea.

La sentenza aggiunge una nota essenziale: nessuna legge o regolamento impone alla banca un obbligo di monitoraggio preordinato alla sospensione di pagamenti anomali (per importo/frequenza). In assenza di parametri normativi la scelta discrezionale della banca avrebbe l'effetto di rallentare le operazioni a danno dei clienti, in evidente antitesi con gli obiettivi di certezza e celerità dei pagamenti.

In sostanza, l'irrigidimento della responsabilità della banca, pur in un'ottica di tutela del cliente, avrebbe l'effetto di paralizzare il sistema. Col progredire dei sistemi e l'incremento delle allerte, il

paradigma della responsabilità oggettiva della banca, prima quasi granitico, tende ad affievolirsi e il contegno assunto dal cliente andrà vagliato caso per caso.

Roberto Pavia