La **sicurezza** è in mano alle ***banche***

CON LA PSD2 LA SICUREZZA DIVENTA UN ASPETTO ANCORA PIÙ CRITICO PER IL BANKING: E DOPO I TANTI INVESTIMENTI, L'APERTURA ALLE TERZE PARTI POTREBBE MINARE L'AFFIDABILITÀ DEL SISTEMA BANCARIO. MA L'OSTACOLO PUÒ DIVENTARE UN'OPPORTUNITÀ

La mia banca è affidabile? Questa percezione sarà sicuramente messa in crisi con il nuovo ecosistema dettato dalla PSD2. «L'apertura del processo di pagamento alle terze parti (TPP), voluta dal legislatore per favorire la competizione tra più soggetti, porterà ad ampliare il numero di realtà coinvolte nella catena del pagamento e quindi, inevitabilmente, ad aumentare i punti vulnerabili con breach – spiega Dario Bonavitacola, Responsabile Infrastrutture Tecnologiche, Servizi e Sicurezza del Gruppo Cedacri. Le terze parti, inoltre, non apparterranno al settore bancario che da tempo invece investe nella sicurezza, ma saranno aziende di "contatto", rivolte a massimizzare l'efficacia del rapporto con il consumatore, producendo software orientati all'usabilità e all'engagement del cliente piuttosto che alla sicurezza».

Dario Bonavitacola, Responsabile Infrastrutture Tecnologiche, Servizi e Sicurezza del Gruppo Cedacri

Influenzare il mercato, per essere sicuri

Eventuali violazioni o attacchi alle terze parti non bancarie si ripercuoteranno quindi sulla percezione di affidabilità di tutto il sistema bancario. Ma questa minaccia può essere trasformata in opportunità. «Se le banche sapranno guidare i clienti verso la giusta percezione di sicurezza, ovvero come un valore che può essere custodito solo da chi ha investito nel tempo in strumenti e processi – osserva Bonavitacola –, potranno avere un vantaggio competitivo sui nuovi soggetti terzi. Ad esempio, influenzando il mercato così da adottare meccanismi di autenticazione di tipo OpenID e Outh2, piuttosto che modalità embedded che lascerebbero parte della catena di sicurezza in capo alla terza parte».

Un approccio integrato

Ma senza dimenticare la qualità dell'esperienza utente. «D'altronde nella quotidianità siamo obbligati a scegliere password "complesse" per rendere l'accesso a un sistema più sicuro – premette Bonavitacola – ma paradossalmente per essere ricordate vengono appuntate su un monitor, compromettendone la sicurezza. È quindi necessario agire sulla end point security mobile e web. E rendere questi punti di accesso sicuri senza gravare sulla esperienza utente: non basterà però agire sui livelli applicativi e sugli strumenti legati ai servizi di back end, ma dovrà essere associato un sistema in grado di lavorare sulla componente comportamentale, legata alla sessione di lavoro del cliente, fino ad arrivare alla transaction risk analysis, basata su dati storici e algoritmi predittivi. L'approccio integrato, a strati, sarà l'unica scelta possibile per diminuire i rischi legati alle frodi informatiche».

Se l'attacco è interno

Ancora una volta, chi troverà «il miglior trade-off tra sicurezza ed usabilità – precisa Bonavitacola –, vincerà la sfida aperta dalla PSD2». Senza dimenticare però che sempre più spesso gli attacchi non provengono dall'esterno ma dall'interno dell'azienda. «Le misure di rafforzamento della sicurezza per prevenire breach interni spesso rendono difficile il lavoro quotidiano – conclude Bonavitacola. Alcune realtà stanno quindi cambiando approccio: piuttosto che esasperare le misure volte a impedire che l'attacco interno si concretizzi, si investe su strumenti e processi adatti a reagire il più velocemente possibile ed espellere l'intruso, prima che crei danni significativi».

G.C.