Sicurezza dei sistemi informativi in ambito bancario: la norma e l'uso

Avv. Valentina Frediani, Founder Colin & Partners, esperta in diritto delle nuove tecnologie

Il contesto. Gli attacchi e le minacce informatiche sono in aumento, non è una novità né una sorpresa. Un approccio strategico alla sicurezza dei sistemi informativi nazionali è prioritario a livello politico-istituzionale, anche in ambito europeo. L'esigenza di prevenzione, difesa e pronta risposta ad un eventuale attacco, è onere e vantaggio per gli Stati e per i singoli operatori business. E' già essenziale per alcuni attori che gestiscono servizi e dati core per lo sviluppo dei singoli paesi. Tra essi vi sono senza dubbio gli Istituti bancari.

Cosa dice la norma. La Circolare n. 285 emanata nel 2013 dalla Banca d'Italia, e modificata nel luglio 2015, detta attualmente le disposizioni di vigilanza prudenziale per le banche, prima contenuti nella Circolare n. 263 del 27 dicembre 2006 Il Capitolo 4 contiene obblighi volti a realizzare un sistema informativo sicuro ed efficiente (attraverso l'adozione di misure di protezione e processi interni a presidio della sicurezza delle informazioni e delle risorse informatiche tra cui: effettuare l'analisi del rischio informatico; adottare policy di sicurezza e standard di data governance; definire una procedura di gestione degli incidenti che includa la cooperazione con le forze dell'ordine e con gli altri operatori coinvolti, notificare alla Banca d'Italia o alla Banca Centrale Europea i gravi incidenti di sicurezza informatica. Tutto favorendo un processo di responsabilizzazione ai vari livelli delle funzioni ICT.

In Europa. La direttiva NIS, che non ha ancora terminato il proprio iter di approvazione, costituisce uno degli strumenti attraverso i quali l'Unione Europea intende realizzare il "terzo pilastro" sulla sicurezza., in particolare agendo sul fronte della sicurezza informatica e ponendo tra gli obbiettivi dell'Agenda Digitale Europea la definizione di una strategia di prevenzione e reazione agli attacchi cibernetici; consentire ai singoli stati di condividere segnalazioni di attacchi avvenuti sui territori nazionali e strategie di difesa. L'Italia con il Dpcm 24 gennaio 2013 ed il Dpcm 18 dicembre 2013 si è già mossa in tale direzione, dettando i principi su cui dovranno articolarsi le linee d'azione e gli indirizzi per la protezione cibernetica e sicurezza informatica nazionale.

Perché investire in sicurezza. Anche se la direttiva europea, che includerà misure rivolte anche alle banche (sebbene sarà necessario attendere l'atto di recepimento interno) non è ancora entrata in vigore, alcuni obblighi specifici sono già in vigore in virtù della Circolare 285/13. Un'ottimizzazione dei processi relativi alla sicurezza cibernetica non risponde tuttavia al mero dettame normativo. Come sottolineato dalla Circolare, per le banche, un sistema informativo strutturato e protetto è anche efficiente; consente di sfruttare le opportunità offerte dalla tecnologia per ampliare e migliorare i prodotti e i servizi, accrescere la qualità dei processi di lavoro, contenere il rischio operativo, garantendo così continuità, integrità e affidabilità.