15° Workshop CIPA – Innovazione IT e banche

9 giugno 2026

La Cybersecurity nel settore bancario in un contesto geopolitico complesso

Saluto di apertura del Presidente

Buongiorno, rivolgo a tutti i partecipanti un cordiale saluto di benvenuto al 15° workshop organizzato dalla CIPA che, come lo scorso anno, si tiene in presenza e da remoto.

L'annuale workshop CIPA rappresenta un'occasione di confronto e di scambio di esperienze tra esponenti delle Istituzioni, del mondo accademico, del settore bancario e della Banca d'Italia su tematiche tecnologiche innovative.

Questa edizione affronta il tema della cybersicurezza nel settore bancario, a fronte delle crescenti minacce anche nel mutato contesto geopolitico, con un focus specifico sulle implicazioni che le nuove tecnologie, in particolare l'intelligenza artificiale, hanno in tale ambito.

Negli ultimi anni l'evoluzione è stata rapidissima. I modelli di IA sono passati dalla capacità di produrre codice a partire da requisiti descritti in linguaggio naturale, a quella di individuare e correggere vulnerabilità, fino alla possibilità di generare anche il codice necessario per sfruttarle. Capacità che fino a poco tempo fa richiedevano team altamente specializzati, tempi significativi e competenze rare stanno diventando automatizzate, scalabili e sempre più accessibili.

Questa evoluzione è ambivalente. Per la difesa, l'IA rappresenta una leva straordinaria: può aiutare produttori di software, operatori di infrastrutture critiche e istituzioni finanziarie a individuare difetti con maggiore rapidità, migliorare la qualità del codice, rafforzare i controlli e ridurre i tempi di correzione. Ma le stesse capacità possono essere utilizzate da attori malevoli, aumentando velocità, scala e sofisticazione degli attacchi.

Il punto centrale è il tempo. Tradizionalmente, tra la scoperta di una vulnerabilità e la disponibilità di strumenti efficaci per sfruttarla esisteva un intervallo utile alla difesa. Se questo intervallo si riduce drasticamente, l'asimmetria tra attaccanti e difensori si amplia. Le organizzazioni complesse, e in particolare le istituzioni finanziarie, non possono applicare automaticamente ogni aggiornamento di sicurezza: devono testarlo, verificarne la compatibilità, valutare effetti indesiderati e garantire la continuità dei servizi. Ma durante questo periodo gli attaccanti potrebbero disporre di strumenti basati sull'IA per sfruttare vulnerabilità già note ma non ancora corrette nei sistemi di produzione.

Per questo la risposta non può essere solo tecnologica. Deve riguardare governance, organizzazione, processi decisionali e preparazione operativa. La prima priorità resta quella di conoscere con precisione il proprio patrimonio tecnologico. Non è possibile proteggere ciò di cui non si conosce l'esistenza. Servono informazioni aggiornate e affidabili sui sistemi critici, sui software utilizzati, sulle dipendenze, sui fornitori, sulle componenti esposte verso l'esterno e sulle interconnessioni tra ambienti.

La seconda priorità è rafforzare i processi di gestione delle vulnerabilità. Dobbiamo prepararci a una fase nella quale gli aggiornamenti di sicurezza saranno più frequenti, più numerosi e più urgenti. Questo richiederà processi decisionali più rapidi, criteri di priorità chiari, maggiore coordinamento tra funzioni tecnologiche, business, risk management e vertici aziendali. La velocità diventerà una componente essenziale della sicurezza, ma dovrà essere una velocità governata.

Allo stesso tempo, non possiamo pensare di difenderci con strumenti tradizionali contro attaccanti che utilizzano strumenti nuovi. Le organizzazioni dovranno integrare l'IA nei propri processi difensivi: analisi del codice, verifica delle configurazioni, test di sicurezza, individuazione delle vulnerabilità, valutazione dell'esposizione. Questo non significa sostituire il fattore umano. Al contrario, il ruolo delle persone resterà essenziale per definire gli obiettivi, configurare gli strumenti, interpretare i risultati, validare gli output e assumere le decisioni finali.

Non è prudente attendere l'ampia diffusione dei modelli più avanzati [alla Mythos]. Risultati importanti possono essere ottenuti anche con strumenti già disponibili, purché inseriti in un quadro di governo, controllo e validazione adeguato. La questione decisiva non è quale modello utilizzare, ma come integrarlo nell'organizzazione: con quali dati, per quali finalità, con quali presidi, con quali responsabilità e con quali limiti.

Vi è poi un profilo particolarmente rilevante per il settore finanziario: l'utilizzo efficace dei modelli avanzati può richiedere di condividere con i relativi fornitori non solo codice, ma anche informazioni sul contesto tecnico: configurazioni, dipendenze, interfacce, architetture e presidi di sicurezza. Sono informazioni sensibili, che richiedono tutele contrattuali, tecniche e organizzative robuste.

È ancor più centrale quindi assicurare una gestione accorta delle cd. "terze parti", includendo esplicitamente i fornitori di IA avanzata e le relative infrastrutture cloud, nella consapevolezza che la presenza sul mercato di un limitato numero di grandi operatori di IA potenzialmente depositari di informazioni sensibili su molte organizzazioni critiche può comportare concentrazione e rischi a livello

sistemico. Il DORA oversight framework offre la cornice regolamentare per affrontarli e mitigarli.

La sfida per le funzioni IT sarà duplice: cogliere tempestivamente le opportunità offerte dall'IA per rafforzare la difesa e, al tempo stesso, governare i nuovi rischi che essa introduce. Questo richiederà investimenti mirati, competenze nuove, collaborazione tra funzioni, dialogo con le autorità, attenzione ai fornitori e capacità di assumere decisioni rapide in condizioni di incertezza.

Desidero concludere con un messaggio chiaro. I cambiamenti in atto sono strutturali e difficilmente reversibili. Le organizzazioni che sapranno prepararsi per tempo — conoscendo meglio i propri sistemi, accelerando la gestione delle vulnerabilità, integrando l'IA in modo controllato e presidiando il rischio di terza parte — saranno meglio posizionate per affrontare le sfide che si prospettano.

Con questo spirito, auguro a tutti una proficua mattina di lavori.