Minacce combinate, la nuova frontiera della sicurezza in banca

a colloquio con Maurizio Tondi, VP Strategy & Business Process Support Axitea
a cura della Redazione

Il profondo cambiamento in corso nel sistema bancario sta spostando sempre più l'attenzione verso le minacce informatiche o di tipo "combinato". Qual è la vostra visione sul tema?

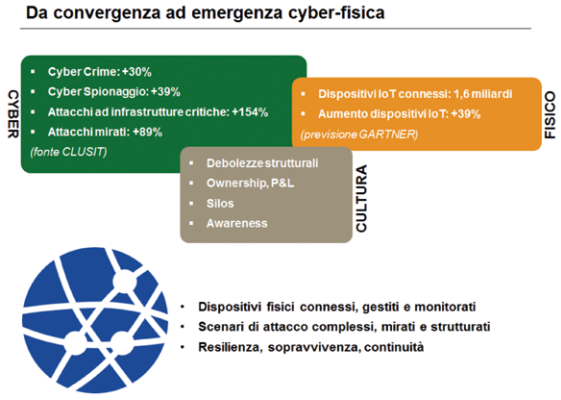
Rispondo facendo una premessa e una domanda: ma i Big Data sono un bene o no? Dipende certamente dal campo di applicazione. Per chi deve, in una Control Room, in un Security Operation Center o all'interno di un CERT (Computer Emergency Response Team) o CSIRT (Computer Security Incident Response Team) gestire con tempestività, accuratezza ed efficacia migliaia di allarmi provenienti da decine di migliaia di sensori, stati dinamici ed informazioni multidimensionali in tempo reale, potrebbero essere un problema. Vale per ogni tipologia di industria e, certamente nel settore bancario dove la ricchezza di informazioni è strumento di grande qualità per la gestione del Cliente. Tuttavia disporre non tanto di una grande mole di dati, ma di quelli "giusti" e delle corrette correlazioni tra informazioni critiche - che provengono da domini fisico-logico ancora separati basati su tecnologie multivendor, nella complessità ed eterogeneità tecnologica delle infrastrutture di servizio delle Banche - è certamente la modalità più efficace per garantire qualità di servizio e di intervento. Evidentemente anche la Banca è "mission critical" da questa prospettiva; non solo, quindi, per la dipendenza del sistema transazionale, dove la riduzione del down time è cruciale, ma data la natura del servizio, dove la tempestiva gestione degli incidenti, degli eventi ed il relativo reporting è parte della gestione del rischio. E' qui che l'utilizzo di piattaforme moderne ed innovative per la gestione di situazioni di emergenza - **Situation Management** - può semplificare e rendere più efficace le modalità di gestione di allarmi e di intervento nel contesto di un CERT, iniziando da una corretta definizione delle SOPs (Standard Operating Procedures) degli operatori impegnati nella supervisione e nel controllo della sicurezza delle agenzie, delle filiali e delle persone. Una questione di "informazioni" ma anche di infrastruttura tecnologica per garantire continuità di servizio, sicurezza, integrità e protezione. In un contesto in cui la convergenza, se non l'integrazione tra impianti di sicurezza fisica e sistemi per la protezione informatica è evidente, oltre che necessaria. Le minacce e gli attacchi sono, infatti, sempre più sofisticati e trasversali e si basano su piani di penetrazione articolati per sfruttare vulnerabilità del domino fisico e di quello logico indifferentemente. Da sempre la Banca è un target preferenziale del cyber crime dove si concentrano ed intrecciano -

con modalità differenti che sfruttano competenze anche differenti ma che sono animate dallo stesso obiettivo criminoso - frodi, estorsioni, sottrazione di informazioni critiche, furti di identità digitali, ATM malware, fino ai più recenti spear phishing, APT (Advance Persistent Threats) e social media. Botnet e sistemi distribuiti sono in grado di lanciare sofisticati DDoS (Distributed Denial-of-Service) per inibire il servizio di una Banca a meno che non venga pagato un riscatto; attacchi ai social media attraverso falsi profili e account compromessi possono agevolmente ottenere informazioni mediante social engineering; mail falsificate ad-hoc provenienti dall'organizzazione o da colleghi possono indurre al rilascio di informazioni riservate e sensibili; codice malevolo che colpisce gli ATM prelevando denaro o manipolando transazioni (ad esempio: Ploutus, Tyupkin, GreenDispenser). Ma anche i non meno dannosi e pericolosi attacchi fisici agli ATM con più o meno sofisticati strumenti che, oltre alla sottrazione del denaro, provocano danni alle strutture ed evidentemente possono contribuire a creare un clima di insicurezza per il Cliente nella fase di interazione con l'ATM di agenzie sempre meno presidiate.

Quali sono le risposte che un Global Security Provider come Axitea può offrire alle mutate esigenze del sistema bancario?

Se il profilo di attacco è realmente integrato ed è strutturato per sfruttare tutte le debolezze dello spazio cyber-fisico, nonché quelle spesso più rilevanti dell'essere umano, la risposta deve essere necessariamente adeguata a questa escalation, a questo pericoloso innalzamento di profilo. La base è, innanzitutto, una **visione integrata** che includa consapevolezza, competenza e "cultura" della sicurezza da parte del personale; **metodologie innovative** per la gestione e valutazione del rischio e per la gestione programmata degli interventi, anche quelli manutentivi che possono mettere a rischio l'integrità o il funzionamento di un sistema od offrire un punto di ingresso nel sistema compromettendo così la sicurezza di informazioni ed asset critici. Pensiamo agli attacchi a qualche Banca internazionale portati attraverso le credenziali di accesso poco protette di un sistema di HVAC (Heating, Ventilation and Air Conditioning) con danni anche rilevanti in termini di immagine. Le minacce stanno emergendo come mai si era registrato fino ad oggi e, spesso, a ciò si aggiunge una debolezza strutturale nella gestione integrata della sicurezza da parte delle Aziende, per natura guidate dal business, dal P&L e dall'accettazione della "forza maggiore" e della "conformità normativa". Dall'evidenza che tutti gli attacchi del passato conosciuti, si sono dimostrati "trasversali" e hanno coinvolto elementi informatici, fisici, umani ed organizzativi, emerge definitivamente la necessità di un **approccio olistico** ed integrato, per essere efficaci nella riduzione dei rischi. L'approccio a "silos" per la sicurezza fisica, informatica e per la protezione del capitale umano si è rivelato assolutamente insufficiente ed inadeguato. Ed in ultimo, ma certamente non meno importante, la disponibilità di **piattaforme tecnologiche** abilitanti e soluzioni per la gestione integrata della sicurezza della Banca. Axitea è, quindi, convinta che un approccio orientato alla "full security" possa coniugare e fondere in un'unica proposizione i servizi awareness (attraverso adeguata formazione, specializzazione e certificazione del personale coinvolto nelle procedure di sicurezza), le metodologie (un approccio di tipo olistico con attività ad esempio di assessment e penetration test attuate su tutto lo spazio cyber-fisico per supportare la Banca nella individuazione di potenziali punti di vulnerabilità ed attuare immediate procedure di remediation) e le soluzioni tecnologiche avanzate, come la realizzazione di un sistema di Situation Management. Per Axitea - che integra sia competenze e prerogative tipiche dell'istituto di vigilanza, centrali operative ed una consolidata esperienza nelle gestione degli allarmi e degli interventi, sia competenze specialistiche nella scouting tecnologico, nella progettazione, realizzazione e manutenzione di impianti di sicurezza anche complessi e personalizzati - la parola chiave è **"life cycle"**: una gestione continuativa della postura di sicurezza delle Aziende adeguata all'evoluzione delle minacce, modulata sul profilo di rischio ed in grado di evolvere secondo le esigenze ed i requisiti del "sistema" del cliente.

In che modo sviluppate il modello di Situation Management per una Banca?



In questo contesto anche la progettazione, la realizzazione o l'integrazione di un Situation Management, che nel caso delle Banche può essere l'asset tecnologico a supporto dell'organizzazione e dei processi sui cui opera il CERT, può avere elementi cruciali già inizialmente, nella fase di assessment dove è fondamentale effettuare una verifica a tutti i livelli dei potenziali e reali punti di vulnerabilità dell'azienda (varchi, ingressi, mezzi di trasporto, parcheggi, personale aziendale, fornitori, partner, sistemi informativi aziendali, sistemi tecnologici, dispositivi fissi e mobili, procedure, etc.) e di realizzare l'immediata messa in sicurezza di asset fisici, dati, infrastrutture, know-how, proprietà intellettuali, personale chiave, attività mission critical e di definire e implementare un processo di manutenzione continuativa focalizzato sul miglioramento e sul mantenimento del livello complessivo di sicurezza della Banca. Viceversa la presenza di sistemi legacy e modalità operative stratificate devono essere valutate con attenzione: le prime in termini di interoperabilità, flussi ed alimentazione di dati, informazioni, stati e segnali che devono - adeguatamente trattati e normalizzati - raggiungere i cruscotti operativi del Situation Management; le seconde per determinare con efficaci procedure standard che rappresentano, a fronte del rilevamento ed acquisizione di un allarme, la baseline comportamentale degli operatori, elementi cruciali per la gestione degli interventi con precisione, efficacia e misurabilità. Anche in funzione dei KPI di servizio che sono stati definiti e delle necessità di reportistica e compliance che le Banche in primis devono osservare. Il Situation Management - come piattaforma software aperta, scalabile e modulare - è in grado di correlare diversi sistemi e sensori e molteplici domini (customer service area, ATM, data center, cash vault, computer, rete, punti di accesso, porte, gate, etc.) consente di avere quindi in ogni momento il quadro complessivo della situazione, la gestione facilitata con procedure operative e, attraverso l'utilizzo di Business Intelligence Analysis (BIA), il supporto intelligente alle decisioni, il supporto intrinseco al filtraggio di informazioni, il riuso di sistemi di sicurezza e safety preesistenti, procedure di escalation e di collaborazione strutturata tra i diversi livelli gerarchici. Ciò si traduce in una maggiore efficienza nel processo decisionale (diminuzione degli errori) in scenari di emergenza e di routine, gestione delle risposte agli eventi critici con continuo miglioramento dell'intervento e riduzione del tempo di trattamento degli incidenti/eventi ed il completamento del ciclo con la creazione di report, training e simulazioni per migliorare il sistema e aumentare le performance delle procedure e la mitigazione complessiva del rischio.