Aumentano gli attacchi agli ATM: le soluzioni AXIS per le banche

a colloquio con Pietro Tonussi, business developer manager Southern Europe Bank Market
a cura della Redazione

Il denaro contante verrà ancora utilizzato nel 2020? Nonostante ci si trovi in un mondo sempre più tecnologico, in cui le transazioni economiche possono essere effettuate attraverso i nostri smartphone e una semplice connessione internet, oppure utilizzando le tradizionali carte di credito, di debito o altri sistemi elettronici, sentiamo ancora l'esigenza di pagare con il cash.

Le persone continueranno a utilizzare denaro contante per una serie di vantaggi (reali o percepiti), tra cui il fatto di credere di usufruire del sistema di pagamento più sicuro, perché non hanno bisogno di una connessione Internet (pensiamo a tutte le aree del mondo, ma anche dell'Italia, in cui si verifica il cosiddetto "digital divide", la differente possibilità di accesso al Web), perché possono effettuare pagamenti senza un intermediario, non ci sono costi di transazione ed è più facile tenere sotto controllo la propria disponibilità economica, o ancora perché è anonimo e non si corre il rischio di furti di identità. In sintesi, l'utilizzo del denaro contante viene percepito dalle persone come semplice, pratico, efficace, veloce e non costoso, tutti fattori che giustificano questi risultati e le stime sul suo utilizzo fino al 2020.

Questo comporta una serie di conseguenze che devono essere tenute in considerazione con sempre maggiore attenzione da chi si occupa di sicurezza nel settore delle banche e degli istituti finanziari. Innanzitutto la presenza di più sportelli ATM sul territorio, ma anche più luoghi per il loro posizionamento (anche in aree non convenzionali come i centri commerciali, aeroporti e stazioni). Questo significa più cash in circolo e di conseguenza maggior rischio non solo per il denaro stesso, ma anche per i clienti e per tutto quello che concerne il prelievo di contante dai bancomat.

Analizzando in maniera più approfondita questa situazione si evince come anche i criminali, sempre più esperti e senza particolari scrupoli, conoscano questa tendenza generale e si siano organizzati di conseguenza per mettere in atto i loro intenti nei confronti delle banche, delle singole filiali e soprattutto degli ATM, con tecnologie e azioni sempre più evolute che si concretizzano negli attacchi ai bancomat che rappresentano il bersaglio preferito.

Secondi i dati del Rapporto Intersettoriale sulla Criminalità predatoria di ABI-OSSIF, è infatti in crescita l'aumento complessivo dei reati predatori, come dimostra l'alto numero di denunce all'Autorità giudiziaria dei furti e delle rapine, rispettivamente +2,2% e +2,6% nel 2014 rispetto al 2013; l'altro dato importante è che **crescono di anno in anno gli attacchi agli ATM bancari**: solo nei primi 9 mesi del 2014 sono stati registrati 433 episodi rispetto ai 321 del 2013, pari a un **incremento del 34,9 %**. Questi atti criminosi **rappresentano inoltre circa l'80% degli attacchi totali**, a testimonianza di come gli ATM siano diventati il **primo obiettivo in assoluto dei malviventi**, in primis proprio per la loro funzione di erogatori di denaro contante.

Con riferimento alla tipologia di attacchi agli ATM,

questi possono essere divisi in due categorie principali: quelli "fisici", dove i criminali intervengono direttamente sul bancomat e quelli "software", come ad esempio il fishing, ovvero la frode telematica. Gli strumenti più utilizzati negli attacchi fisici sono i gas/esplosivi, le seghe a disco, la dinamite, i martelli e altri arnesi da scasso. Il "cash trapping" risulta il sistema preferito dai malviventi per rubare i soldi dal bancomat, perché è il più semplice da applicare e non richiede particolari conoscenze informatiche. Tra le modalità di attacco fisico più utilizzate ci sono indubbiamente quelli con gas e/o esplosivi, ma è lo skimming quello che spesso ha conseguenze più gravi per il malcapitato soggetto che subisce la truffa. Dobbiamo infine suddividere gli **ATM in due categorie a seconda della loro locazione**: *on-site*, vicino all'agenzia o in area self, normalmente il locale adiacente alla filiale, oppure *off –site*, quelli installati in centri commerciali, aeroporti, stazioni e simili, questi sono quelli chiaramente più soggetti a vandalismi di ogni genere.

"Di fronte a numeri di questo tipo e ai dati sugli attacchi che sono in aumento, bisogna tenere in considerazione anche l'impatto emotivo che viene provocato nel soggetto che subisce, ad esempio, una rapina mentre sta prelevando – aggiunge Pietro **Tonussi, Business Developer Manager Banking Southern Europe di Axis Communications** – *è fondamentale tutelare la sicurezza dell'individuo, rispettando nello stesso momento la sua privacy. Le telecamere quindi vanno viste come oggetti per la sicurezza e la salvaguardia dell'assett aziendale (il bancomat) ma anche e soprattutto di safety, vale a dire per assicurare efficienza e una migliore assistenza ai clienti.*

La videosorveglianza IP come soluzione

Le linee guida per arginare queste tipologie di attacchi sono fondamentalmente tre: l'utilizzo di sistemi di riprese (videosorveglianza), l'uso di controlli biometrici e la geolocalizzazione dei valori, vale a dire la possibilità che il bancomat o il deposito cash possa essere referenziato in modo geografico. Axis Communications, leader di settore della videosorveglianza IP, dispone nella propria gamma prodotti di telecamere di rete adatte ad affrontare questi tipi di attacchi e può essere davvero considerato il partner ideale per

gli istituti bancari nel garantire la sicurezza degli ATM. Tra le telecamere IP che possono apportare un notevole contributo al mondo bancario ci sono sia quelle per il controllo area, che fanno della qualità di immagine e della supervisione a 180° il loro punto di forza, sia quelle che si possono sistemare nei pressi o nel bancomat, come le *pinhole* dalle dimensioni super compatte, e dalle grandi prestazioni con video HDTV. I sistemi video di rete Axis, oltre ad una videosorveglianza di alta qualità, possono migliorare l'assistenza ai clienti (safety) e facilitare le varie attività ottimizzando i costi. Innanzitutto grazie alla sorveglianza di tutta l'area circostante lo sportello, con l'utilizzo di telecamere panoramiche a 360° che consentono di sorvegliare in modo completo e con l'ausilio di una sola telecamera l'area, eliminando gli angoli ciechi. Le telecamere HDTV con obiettivo pinhole, montate all'interno degli sportelli automatici, installate in modo appropriato, possono garantire un elevato dettaglio della scena interna all'ATM con immagini di eccezionale qualità, anche in ambienti con condizioni di illuminazione difficili, come in presenza di grandi finestre o ingressi con porte in vetro e pavimenti lucidi. In definitiva le prime telecamere, utili per il controllo d'area generano overview, mentre le seconde catturano i dettagli, realizzando un break-even ideale tra privacy e safety del cliente. Offrono inoltre il notevole vantaggio di poter essere integrate con sistemi di allarme e di controllo degli accessi, anche da remoto, per una piattaforma di sicurezza completa ed efficiente.

Secondo una survey del 2014 realizzata da **ATMIA**, associazione no-profit che si occupa di analizzare l'universo degli ATM a livello mondiale, risulta che **ci sia una presa di coscienza da parte dei manager responsabili della sicurezza bancaria sull'importanza delle soluzioni tecnologiche**, come la videosorveglianza IP, nell'affrontare il problema degli attacchi agli ATM. Apparentemente, l'inserire ulteriore tecnologia in impianti esistenti potrebbe essere percepito come un costo aggiuntivo, ma teniamo presente che, quando dei criminali attaccano un ATM, la banca affronta dei costi ben superiori che non sono solo quelli del bancomat danneggiato, ma possono essere anche i danni alla struttura del palazzo che la ospita, eventuali feriti tra i passanti o - nella peggio-

re delle ipotesi - delle vittime. "*Inoltre, non possiamo dimenticarci di altri fenomeni che spesso accadono all'atto del prelievo:*– continua **Tonussi di Axis Communications** – *Se un cliente subisce una rapina dopo aver prelevato a uno sportello bancomat, quella filiale non avrà un danno diretto, ma avrà perso un cliente che non si sentirà sicuro ad effettuare questa semplice operazione. L'impatto emotivo sul cliente potrà essere ancora più grave perché andrà ad influire a livello di "customer insatisfaction", elemento che nel futuro una banca dovrà tenere sempre più in considerazione per fornire un servizio all'altezza e per migliorare l'assistenza ai clienti (safety).*

Un altro scenario assai tipico è quello di un utente che si reca in un'area self e vuole prelevare del denaro contante: ci sono due possibili situazioni che possono provocare un danno diretto o indiretto alla banca. Partiamo dalla prima: il cliente può trovare all'interno dell'area self un senzatetto che ha scelto di dormire in questo luogo perché è un posto caldo, in grado di offrire riparo dalle intemperie esterne; il risultato sarà che il cliente non entrerà a prelevare perché non si sentirà al sicuro, creando così un danno indiretto alla banca. Immaginiamo ora che un soggetto entri nell'area self e si senta improvvisamente male, accasciandosi a terra: senza un adeguato sistema di videosorveglianza la banca non è in grado di assicurare la sicurezza del cliente nel modo migliore (danno diretto). Due situazioni diverse, che esemplificano come grazie ad algoritmi intelligenti che rilevano la presenza di un uomo a terra, in grado di riconoscere se un uomo è in posizione orizzontale perché sta dormendo oppure perché sta male, la banca abbia a portata di mano una soluzione utile a garantire la compresenza di safety & security. Una stessa analitica che le banche desiderano per limitare un possibile problema, che può verificarsi anche in altri ambienti oltre a quello delle aree self degli ATM. Le soluzioni Axis, grazie ad allarmi antimanomissione e alla funzionalità di rilevamento di oggetti, nonché ad applicazioni di partner di Axis come quella appena enunciata, permettono di identificare rapidamente anche potenziali attività di skimming e trapping di banconote e carte o altre attività criminose ai danni dei bancomat.

E quando si verificano attacchi con gas esplosivi o con altri attrezzi da scasso? Anche in questo caso la videosorveglianza IP può tornare utile alla banca. Pensiamo innanzitutto a cosa succede in questi casi e a quale sia il comportamento umano dei criminali che effettuano un attacco di questo tipo, per comprendere come la tecnologia possa risolvere questo problema. Sicuramente un criminale che deve far esplodere una cassaforte non avrà un atteggiamento tranquillo come potrebbe essere una persona che deve semplicemente prelevare. Le statistiche su questa tipologia di attacchi evidenziano inoltre che sono ancora due i gas più utilizzati dai malviventi: l'ossigeno e 'acetilene. Innanzitutto perché sono entrambi inodore e non vengono rilevati dai nasi elettronici. L'ossigeno, inoltre, viene scelto perché deflagra senza fuoco, preservando dalle fiamme le banconote, che altrimenti sarebbero inutilizzabili. Le statistiche evidenziano come gli attacchi fisici siano quelli più perpetrati ma, come abbiamo detto, è possibile **realizzare con le telecamere un'analisi comportamentale**, perché c'è sempre una certa concitazione in questi gesti, tipica di questi attacchi: l'analitica è appunto in grado di rilevare tali movimenti, offrendo così la possibilità di attivare delle azioni quasi immediate di fronte a un potenziale gesto criminale o segnalare un potenziale caso sospetto.

Sul piano degli attacchi fisici si dovrebbe in ogni caso ricorrere di più alla **deterrenza a scopi preventivi** che si può ottenere in due modi: con le telecamere sistemate nell'area esterna al bancomat, che possono scoraggiare i criminali nell'attuare determinate azioni, ma soprattutto con telecamere che possono essere utilizzate anche all'interno del bancomat per andare ad analizzare le scene che potrebbero essere sospette, ad esempio relative a persone che hanno effettuato uno o più sopralluoghi nei giorni precedenti all'attacco dell'ATM.

Infine, se analizziamo i dati sugli attacchi agli ATM forniti da OSSIF-ABI e ATMIA e visti i numeri di atti criminali perpetrati a danno delle banche, se ne desume che nonostante cresca la percezione dell'importanza di queste tecnologie nel prevenire e garantire la sicurezza degli ATM e delle filiali in generale, esse non sono ancora così utilizzate in maniera capillare. "Capisco che sia inevitabile dover fare dei confronti tra investimenti e contenimento dei costi, ma un terzo elemento deve essere preso in considerazione quando si prendono decisioni di questo genere, che è la sicurezza del cliente, che ogni giorno usufruisce dei servizi che la banca offre", conclude Tonussi.