Banche e Sicurezza 2017 (2): ai rapinatori non piace la guardia, anche se virtuale

a cura di Raffaello Juvara

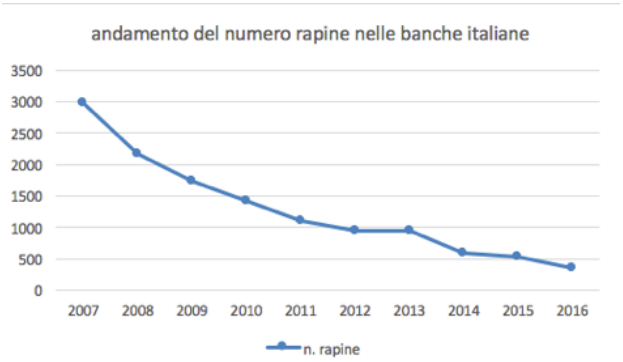
In occasione di **Banche e Sicurezza 2017** (Milano, 23-24 giugno), sono stati resi noti i dati relativi alle rapine in banca nel 2016, che si sono fermate a 360, con una riduzione del 90% rispetto al 2007. In questi dieci anni, l'indice di rischio è sceso da 9,1 a 1,2 rapine per 100 sportelli, mentre le rapine fallite sono passate dall'11,7% al 34,1%. Il bottino complessivo si è ridotto da 57 milioni di euro a 10,6 complessivi, pur registrando un aumento consistente del bottino medio (da **19.328 a 29.538 euro**).

Un altro dato saliente del 2016 è stata l'assenza di rapine in 38 province, con una concentrazione degli episodi conclusi in 19 con Roma e Milano in testa che, peraltro, hanno registrato nel decennio riduzioni in linea con la media nazionale.

Infine, le rapine commesse nel primo trimestre del 2017 sono state 52, segnando un ulteriore dimezzamento rispetto all'anno precedente.

Giovanni Gioia (OSSIF), che ha presentato questi dati, ha indicato alcune ragioni di un risultato tanto eclatante, fra le quali la collaborazione sempre più stretta con le forze dell'ordine, le diverse modalità di gestione del contante e la diffusione di sistemi tecnologici per la difesa delle agenzie. Gioia ha concluso citando **Peter Orszag**, il sociologo consigliere del presidente USA Obama, che aveva sostenuto che per i malviventi sia un deterrente più efficace la consapevolezza di venire scoperti e arrestati che la lunghezza della detenzione in carcere.

Anche **Andrea Coana (Banca Sella Holding)** ha analizzato il fenomeno della riduzione delle rapine, partendo dal confronto dei dati a livello europeo, che dimostrano che la riduzione del 90% registrata in dieci anni ha riportato l'Italia nella media,



dalla quale si era clamorosamente allontanata con i picchi del 2007 e degli anni seguenti. Entrando nel dettaglio delle misure di prevenzione che hanno agito con efficacia, Coana ha citato l'adozione generalizzata delle porte a bussola, delle centrali operative di proprietà diretta delle banche, dei dispositivi di cash-in e dei temporizzatori delle casseforti, unitamente alla formazione del personale ma, in particolare, si è soffermato sugli effetti psicologici di alcune misure come, ad esempio, la "guardia virtuale".

Utilizzando un video ripreso dalle telecamere di un'agenzia, che documenta la rinuncia a commettere una rapina da parte di due malintenzionati che si sono accorti, prima di entrare nei locali, del funzionamento dell'applicazione, Coana ha sottolineato l'efficacia deterrente della consapevolezza di "trovarsi in scena", prodotta dalla comunicazione adeguata di quanto sta accadendo in quel momento nell'agenzia.

"La guardia virtuale stabilisce una relazione univoca con gli utenti, si sentono continuamente parte di una scena – ha concluso Coana – come oggi avviene a livello generalizzato con l'uso dei social".

Abbiamo chiesto a **Nils Fredrik Fazzini, general manager di Citel spa**, l'azienda che ha sviluppato l'applicazione della "guardia virtuale" più diffusa tra le banche italiane, di approfondire l'argomento per i nostri lettori illustrandoci il punto di vista del costruttore specializzato, che cosa c'è dietro le apparenze e cosa ci aspetta dietro l'angolo. Un'occasione importante, perché la sensazione che affiora è che si stia materializzando un modo nuovo di fare sicurezza fisica, che va ben oltre il PSIM e i suoi 7 criteri: qui ci si rende conto che la sicurezza fisica è un processo sempre più somigliante a un processo gestionale appartenente ad un sistema informatico real time gestito a livello dipartimentale da un utilizzatore con un ruolo del tutto allineato a quello di altri servizi aziendali dotati di un sistema informatico per l'operatività efficiente e compliant.

per gentile concessione di Axitea

Nils, qual è stato il ruolo di Citel, nell'esperienza degli utenti delle banche italiane, che ha ridotto in modo così clamoroso le rapine? E In che misura incide il PSIM, la tecnologia citata più volte durante Banche e Sicurezza 2017 come esempio di "misura efficace" per la diminuzione degli attacchi?

Il fatto essenziale è che le banche italiane – già detentrici di record mondiali non lusinghieri per le rapine subite – hanno ottenuto nell'ultimo decennio un abbattimento del 90% del numero di casi grazie proprio alla progressiva adozione di misure innovative di dissuasione e di limitazione del danno in sostituzione o ad integrazione delle protezioni fisiche tradizionali. E quasi sempre rinunciando al presidio armato della vigilanza in loco, i cui costi risultavano per la banca sempre meno sostenibili.

Il contributo evolutivo di Citel in un arco di tempo ultradecennale è stato il salto di qualità rispetto ai primi esempi di guardia remota, rudimentali perché si limitavano a un video bidirezionale e alla possibilità di chiamare una cosiddetta "video-bonifica" e di ottenere l'attivazione di tele-consenso per l'apertura di una cassaforte.

Oggi siamo a un livello di ingegneria e di software di un'altra dimensione: al posto della guardia e delle corazze delle casseforti oggi opera un'intelligenza diffusa e impalpabile che nel tempo si è progressivamente evoluta combinando tecnologie e processi interattivi e che si rivela in tutta la sua efficacia con il crollo delle rapine nelle statistiche.

Un'intelligenza, peraltro, che è tale anche perché porta a rendere l'accesso alla banca controllato ma non complicato, e perché interagisce con il visitatore per rassicurare il cliente e per dissuadere il malintenzionato.

Quindi, dietro il crollo delle rapine non ci sono soltanto gli aspetti visibili a tutti, come l'immagine della Control Room di controllo e gli erogatori blindati del cassiere, ...

Assolutamente no. I progetti degli ultimi 5/6 anni si sono concentrati volutamente sui processi di automazione, ovvero sulle funzioni software di integrazione e correlazione nella catena operativa, fino alla possibilità di usare le tecniche predittive basate sui grandi numeri per ottimizzare la reazione. A prendere in carico il visitatore oggi sono processi che appartengono ad una sistemistica d'insieme, sulla quale c'è stato nell'ultimo decennio un importante lavoro di ingegneria da parte di Citel con la collaborazione determinate con le principali banche italiane, per l'affinamento progressivo di processi software per ottenere in campo funzioni intelligenti, ovvero contestualizzate e combinate con l'informatica di sportello e sotto la supervisione di una Control Room che viene coinvolta in modo mirato dagli stessi processi periferici.

Siamo dunque tornati ai processi invisibili che prevalgono sul visibile?

Si sta percorrendo la strada della migliore combinazione tra il visibile che è appariscente e tecnicamente banale e l'invisibile, che non appare ma che richiede spesso l'intelligenza ottenuta dall'esperienza.

Nella fattispecie l'intelligenza basilare riguarda l'interazione tra apparati, a un livello superiore l'intelligenza è quella delle correlazioni di segnali e di protocolli, mentre al livello massimo l'intelligenza non risiede più in campo ma al livello del sistema di supervisione, in grado di generare non solo eventi ma anche *situazioni*, e non solo su dati di fatto ma anche su basi predittive.

A livello di PSIM, quindi, si stanno raggiungendo livelli di conoscenza specialistica che scaturiscono dall'esperienza specifica e dalla sua accumulazione organica, per passare poi alla sua elaborazione ed al riversamento continuo nell'applicazione. E a questo punto non posso trattenermi dal chiosare questa precisazione con un "si fa presto (oggi) a dire PSIM", senza considerare i contenuti di esperienza che devono essere incorporati in una applicazione informatica da cui ci si aspetta l'erogazione di processi gestionali professionali.

Nella pratica si tratta di **processi invisibili** per il rilascio pilotato del contante e/o per attivare visualizzazioni **volutamente espressive** come l'immagine di una Control Room con operatori impegnati nel controllo, oppure di una guardia professionale che dal video ricorda ai presenti i rischi che si corrono a fronte dell'eventuale magro bottino di una rapina. Mentre, se l'ambiente è tranquillo, lo stesso schermo può essere sfruttato per l'invito rivolto al cliente perché prenda in considerazione i vari prodotti finanziari della banca e le eventuali campagne promozionali in corso.

I passi da gigante fatti dall'epoca dei primi progetti di guardia remota fino alle realizzazioni più recenti non sono quelli visibili sugli schermi dissuasivi in filiale, ma quelli che stanno dietro lo sviluppo di processi di generazione degli *eventi* e delle *situazioni*, per i quali finalmente le piattaforme di correlazione professionali si sono rivelate indispensabili. Lo dimostra l'impennata nella richiesta delle nostre piattaforme di gestione eventi nel settore bancario, appunto per la sostituzione delle centrali di allarme tradizionali, spesso inadeguate per il nuovo contesto.

Questo vuole dire che l'innovazione si estende anche alle piattaforme in campo?

In effetti le vere innovazioni di processo per la sicurezza fisica stanno nelle funzioni di correlazione e di interoperabilità che interagiscono banalmente con un contatto magnetico, ma anche e soprattutto con l'intelligenza degli apparati erogatori, dei CICO in particolare ma non solo, per mettere al sicuro i versamenti e comandare le attuazioni di rilascio di denaro solo in presenza di chi ne ha titolo.

In definitiva, per minimizzare il bottino del rapinatore che ha fretta e per dissuadere il malintenzionato pronto a compiere una *rapina lunga*, oppure chi sta compiendo un sopralluogo per un progetto di rapina in prospettiva.

E cosa pensate della combinazione tra physical e cyber security?

È un'istanza tutt'altro che trascurabile, e non solo in banca. Non la vedo applicabile al caso delle rapine, che sono estemporanee, ma dell'attacco ai caveau basato sull'isolamento informatico del sistema centralizzato di gestione degli allarmi.

Quello che percepiamo, tra i nostri grandi utenti bancari, è l'impressione che gli attacchi ai caveau possano tornare in auge dopo che il fenomeno era stato praticamente azzerato negli ultimi 15 anni grazie alla centralizzazione degli allarmi gestita internamente alla banca.

Non possiamo entrare in dettagli, vista la delicatezza della materia, possiamo solo dire che gli attacchi di successo non hanno mai coinvolto i sistemi di Citel. Aggiungendo che comunque ogni installazione PSIM in banca prevede il superamento dei *penetration test* sulla filiera che va dalla centrale di allarme fino ai server applicativi. Test eseguiti da specialisti incaricati e controllati dalla struttura di Cyber Security della banca, che riguardano le comunicazioni tra PSIM e centrale di allarme, considerando anche quest'ultima come possibile punto di accesso. E non a caso è questo il contesto che ha portato di recente a valorizzare le piattaforme professionali superando quella banalizzazione della centrale di allarmi che ha involontariamente caratterizzato delle scelte del passato.