

# II PSIM in banca

a colloquio con Nils Fredrik Fazzini, Consigliere Delegato di Citel spa  
a cura della Redazione

Nel numero del 17 febbraio della newsletter di OSSIF viene riportata una notizia in evidenza: **“Anche nel 2016 forte calo delle rapine. Le rapine sono state in tutto 298, con un calo del 28,4% rispetto ai primi 9 mesi del 2015 (416 casi). Risulta in diminuzione anche l’indice di rischio, pari a 1,3 rapine ogni 100 sportelli, contro un valore di 1,8 registrato nel 2015. Un decremento sta caratterizzando anche il bottino medio per evento, pari a poco più di 28 mila euro e la percentuale di rapine con un importo rapinato superiore ai 5 mila euro, pari al 65,1%.”**

Forse non sarebbe stato male aggiungere al testo un *“nonostante la drastica riduzione dell’impiego di guardie armate all’esterno o all’interno della filiale per utilizzarle in modo più efficiente nel monitoraggio da Control Room e nella collaborazione con le Forze dell’Ordine.”*

La notizia non era accompagnata da ipotesi sui motivi di un calo di quella portata; ma c’è da chiedersi cosa ci sia dietro questo crollo. Abbiamo rivolto questa domanda a **Nils Fredrik Fazzini**, Consigliere Delegato di **Citel SpA** che, con la sua piattaforma **Centrax-PSIM**, controlla direttamente o indirettamente circa 25.000 tra agenzie bancarie e Uffici Postali in Italia.

**Dal suo punto di osservazione, quali sono le motivazioni alla base della continua diminuzione delle rapine in banca?**

Per Citel i numeri pubblicati premiano giustamente gli investimenti in tecnologia, da parte di Banche e Poste, che hanno alzato di molto l’asticella rispetto all’avversario e ridotto il bottino atteso. Pensiamo alla cosiddetta “Guardia Remota”: quella che in passato si limitava a ricordare da un monitor al malintenzionato che la filiale era video-controllata da un Istituto di Vigilanza e che probabilmente sarebbe stato attivato un qualche intervento immediato sul posto per impedire la rapina. Si trattava di un modo efficace, almeno inizialmente, per scoraggiare la rapina lunga ma, certamente, non quella breve, comunque ancora in uso presso Banche che non hanno fatto – per motivi comunque rispettabili – il passaggio successivo. L’innovazione degli ultimi tempi (che, per la cronaca, vede come protagoniste le Banche che avevano saltato la prima fase), si basa su misure che non si sono fermate alla visibilità ma hanno



elaborato processi avanzati, ormai largamente sperimentati, che comportano **l’integrazione e la correlazione tra tutti i mezzi forti, gli erogatori di contante fino al sistema informatico di sportello**. Non più, quindi, la semplice video-assistenza o video-bonifica da centro di controllo, su richiesta dell’agenzia prima di procedere all’apertura di una cassaforte o a fronte del comportamento sospetto di un cliente.

**Si può quindi parlare a buon diritto di risultati ottenuti grazie all’innovazione tecnologica?**

Le banche più innovative sono passate ormai a **processi in logica PSIM in filiale, con mezzi forti asserviti a un’intelligenza legata a eventi e situazioni ottenute da correlazioni automatiche o semiautomatiche** che, bloccando ogni fonte di erogazione di denaro, spersonalizzano l’interazione tra dipendente della banca e rapinatore, proprio grazie all’evidenza dell’automatismo del processo e dell’inutilità di una qualsiasi forzatura. Facendo aleggiare nel contesto della filiale la presenza di un’intelligenza di governo della situazione senza, peraltro, poterla materializzare, localizzare, né tantomeno forzare o ricattare perché non associabile a una persona fisica, ma a delle funzioni informatiche. E senza dimenticare che una Control Room – che si fa vedere e sentire – monitorizza per prepararsi ad attivare ulteriori misure.

In definitiva, **una condizione di natura prevalentemente informatica, non ricostruibile e non condizionabile**, con l’unica certezza che ad attivarla non è stato l’addetto allo sportello, con una conseguente situazione di impasse per



il malintenzionato, per la certezza di trovarsi oltretutto sotto osservazione da parte di una Control Room.

**Dietro questo processo prevalentemente automatico di gestione dell'evento rapina, c'è il PSIM della Banca, che gestisce questi ed altri processi, in modo sempre più intelligente e discreto; ma anche adattativo nel tempo, grazie all'aggiornamento dei processi e al loro progressivo affinamento.**

Per ottenere questo *adattamento evolutivo* occorre una logica flessibile e riconfigurabile a tutti i livelli, che si stabilisce tra il mezzo fisico e la logica di governo locale per arrivare fino alla logica centralizzata e al feed-back per l'eventuale reazione.

Un modo di operare ormai scontato per l'informatica applicata ai processi aziendali, gestionali e produttivi, ma che si può prestare a imitazioni delle apparenze e della terminologia nel campo della sicurezza fisica, come si è visto con l'improvvisa recente fioritura di proposte PSIM, dopo che Citel lo ha "sdoganato" dalle colonne di *essecome/secuindex*.

Ma se si va fondo, la realtà è ben più complessa e, soprattutto, richiede tempi lunghi di maturazione e quello del PSIM in Banca ne è la conferma.

L'**interazione tra processi** ha come prerequisito l'**integrazione tecnica** tra dispositivi all'interno di una sistemistica adeguata: sia tra centro e periferia che nell'ambito di quest'ultima per i vari sottosistemi che la popolano. Un'**interazione funzionale** richiede scambio di protocolli, sviluppi applicativi e – in definitiva – collaborazione senza riserve e disponibilità a investire in un'ottica di medio e lungo periodo da parte dell'integratore di sistema.

È emblematico, in questo senso, il caso delle **funzioni di correlazione**, spesso trascurate fino ad oggi ma **risultate spesso decisive in questi ultimi anni non solo a livello di PSIM ma anche a bordo delle centrali di allarmi, alle quali ormai non si richiede più di far scattare semplici allarmi, ma di generare eventi e situazioni e di attivare reazioni anche complesse**. E non solo in base a segnali provenienti dai soliti sensori, ma anche da input informatici via protocollo da altri dispositivi, come (parlando di banche) la quantità di banconote presenti in un erogatore o la segnalazione di un *agent* software di un Bancomat, come anche la possibilità di intercettare dal sistema informatico di sportello apposite segnalazioni o time-out, solo per fare degli esempi.

Non si tratta di semplici episodi o proiezioni nel futuro, ma di dati di fatto attualissimi: negli ultimi due anni, Citel ha registrato



un'autentica impennata nelle vendite di centrali di gestione eventi della serie Novax nel settore bancario; guarda caso, proprio ad opera di quelle banche che si sono spinte più avanti nella realizzazione di progetti di gestione integrata dell'evento rapina e non solo. E gli scopi sono quelli appena citati:

- acquisire input sia elementari / tradizionali che informatici;
- correlarli per ottenere tempestivamente eventi attendibili;
- trasferire al sistema di supervisione sia output elementari che informazioni più complesse per ottenere delle reazioni di mitigazione del rischio e del danno secondo procedimenti guidati e tracciati;
- lasciare la gestione agli automatismi locali e alle procedure gestite da Control Room, dove la Guardia Giurata è un operatore che viene indirizzato dalla procedura del sistema per telegestire per eccezione ciò che non è appropriato automatizzare in loco.

**Possiamo affermare, in definitiva, che questo processo evolutivo sia maturato nel mondo bancario con ricadute per le altre categorie di utenti?**

E' vero, ancora una volta si può dire che le Banche italiane sono all'origine delle principali innovazioni di fondo in ambito sicurezza fisica, dal PSIM come paradigma di sistema di gestione alle centrali di correlazione di segnali e protocolli multifunzione, all'affermazione ormai irreversibile dell'uso di reti dati con protocollo normalizzato multifornitore, ad alta resilienza per continuità operativa e protezione del dato.

Per concludere, fatta la rivoluzione infrastrutturale appena ricordata, l'innovazione in banca si è ora spostata sui contenuti funzionali dei *processi di automazione e/o telegestione* degli eventi e delle situazioni per ottenere il massimo della protezione e della dissuasione senza rallentare i flussi operativi e limitando il rischio per dipendenti e clienti.

E forse "il PSIM in Banca" può essere il degno nome di questo passaggio epocale per il settore.

**CONTATTI: CITEL SPA**  
 info@citel.it  
 www.citel.it