

**NUOVI CONCETTI SULLA PROTEZIONE ANTIRAPINA  
DEGLI IMPIANTI BANCOMAT**

P.i. MICHELE MESSINA  
*Dirigente Settore Prevenzione e Sicurezza - ANIA*  
*Vice Presidente A.I.PRO.S.*

**LA SITUAZIONE ATTUALE**

Vista la sempre maggior propensione e familiarità della clientela verso gli sportelli automatici "bancomat", la diffusione di detti strumenti è in costante aumento.

Pertanto nelle casseforti di questi apparati di erogazione si tende a concentrare sempre maggiori quantità di denaro, con conseguente aumento dei rischi e della sinistrosità.

Ogni anno si verificano oltre 200 attacchi, prevalentemente furti, a danno degli impianti "Bancomat", attuati dai criminali, anche in presenza di impianto di allarme, mediante effrazione del battente con l'uso di attrezzi vari, gas ecc. Il danno, in termini di valori assicurati risulta spesso assai rilevante ed è rappresentato, sostanzialmente, da: crollo parziale delle strutture murarie del locale e/o dell'edificio in cui è installato l'impianto; distruzione della componente hard-ware (inclusa la cassaforte); furto delle banconote contenute nei cassetti. Per la banca, il danno è rappresentato principalmente dalla temporanea messa fuori servizio dello stesso impianto ATM, con conseguente disagio per la clientela; da eventuali richieste di risarcimento da parte di terzi, per aspetti di responsabilità civile e, soprattutto, da perdita d'immagine.

Oltre al classico furto notturno, si stanno diffondendo in modo preoccupante, rapine e aperture senza scasso (c.d. misteriose sparizioni) in orario di attività degli sportelli, tanto che, dall'inizio dell'anno, se ne sono contati oltre 80, con ingenti danni economici.

Con preoccupazione, è necessario evidenziare la perdita di efficacia dei mezzi di riferma quali serrature e ritardatori di apertura di varie marche e modelli, ormai ben conosciuti, al punto che i malviventi attendono che trascorra il tempo di ritardo ed il consenso all'apertura, senza paura, tenendo in ostaggio gli impiegati. Viceversa, dove il servizio di rifornimento è esternalizzato a società di vigilanza e trasporto valori, sempre più spesso si verificano le cosiddette misteriose sparizioni, cioè asportazione del contante dai cassetti dell'impianto ATM, senza effrazione del mezzo di custodia.

Queste azioni criminose possono essere imputabili sia ad azioni di specialisti del crimine che avvalendosi di sofisticati e non certo comuni strumenti (endoscopi, ecc.) riescono a "leggere la serratura" ed a ricostruire i profili e le mappe delle chiavi meccaniche, nonché ad individuare l'esatto codice della riferma a combinazione - occorre tuttavia sottolineare che tali strumenti sono di difficile reperibilità e non certo di semplice utilizzo - sia a infedeltà degli addetti.

A seguito di accurate perizie tecnico-assicurative, è stato possibile appurare che in molti casi si sarebbe trattato di infedeltà degli addetti al caricamento i quali, con banali trucchi sono riusciti ad impossessarsi di ingenti quantità di denaro, restando impuniti.

Tra i principali trucchi escogitati, si evidenziano i seguenti:

- non corretta chiusura delle casseforti, che permette così una successiva riapertura senza scasso;
- illecita copiatura di chiavi e codici delle serrature dei mezzi di custodia, fornite poi ai complici che possono così vuotare, senza grosse difficoltà, i cassetti dell'impianto "Bancomat".

Ancora una volta, è dimostrato che l'anello più debole della catena della sicurezza è l'elemento umano!

Analizzando con attenzione i sinistri, risulta evidente che i rapinatori sono quasi sempre ben informati, anche grazie a qualche basista, sono sempre a conoscenza del fatto che la cassaforte è stata appena rifornita di contante, vuoi perché il furgone porta valori e visibile, vuoi perché, più semplicemente, conoscono in anticipo le procedure seguite dagli addetti al trasporto dei valori e la tempistica dei loro spostamenti.

Molte delle misure, tra quelle normalmente adottate per proteggere gli impianti ATM, risultano ormai insufficienti per arginare le rapine e le misteriose sparizioni:

- Il rinforzo meccanico della cassaforte:  
Non ha rilevanza perché non vi è scasso.
- La serratura a ritardo di apertura:  
E' utilizzabile soltanto per ATM installati negli insediamenti della banca e gestiti direttamente da proprio personale. Tuttavia, in parecchi casi, i rapinatori attendono che trascorra il tempo di ritardo, tenendo sotto minaccia i dipendenti.  
N.B. Il servizio esternalizzato non consente di attuare tempi di ritardo di apertura della cassaforte, per ovvie ragioni di costo.
- L'impianto d'allarme:  
Se non gestito in tempo reale da *CDT* e soprattutto nel caso di attivazione e disattivazione locale, affidata agli operatori addetti, è da ritenersi insufficiente.
- La videosorveglianza locale:  
Rappresenta un relativo deterrente; ha funzione di ricostruzione di evento, in caso di sinistro, ma se i rapinatori sono incensurati.....
- Le procedure di sicurezza:  
La mancanza di procedure di sicurezza chiare, ben definite e di accurato, periodico, *audit* interno, aumenta i rischi di furto legati a infedeltà e coercizione degli addetti al caricamento delle banconote.
- Macchiatori del contante?  
Inefficaci in caso di apertura senza scasso, mediante copie di chiavi e utilizzando i codici delle serrature a combinazione.

### **LE SOLUZIONI MIGLIORATIVE PER PREVENIRE I DANNI**

Oggi si parla tanto di ricerca e innovazione, e nel mondo sappiamo essere noi italiani riconosciuti tra i più forti specialisti nel settore della sicurezza e, ahimè..., anche nelle attività criminali; non mancano certo nel settore della sicurezza le aziende in grado di studiare e attuare nuove soluzioni tecnologiche per arginare i suddetti fenomeni criminali.

Quali miglioramenti occorre allora apportare alle attuali difese? Per quanto attiene ai rinforzi, alle blindature e agli ancoraggi non si può fare molto di più di quanto si è fatto finora.

Riguardo ai rischi di rapina e di misteriosa sparizione, una nuova tecnica potrebbe essere quella di tenere sotto controllo, elettronicamente, la quantità di contante deposto nei cassetti dell'impianto "bancomat" in maniera tale che, in caso di rapina o di illecita apertura della cassaforte, non sia possibile sbloccare le serrature del battente del mezzo di custodia, se i cassetti contengono ancora del contante. Questo miglioramento che dovrebbe essere apportato agli impianti esistenti, potrebbe avvenire con estrema facilità ed a costo relativamente contenuto.

Pertanto in termini di nuova strategia di sicurezza, al fine di ridurre i rischi in parola, ritengo sia giunto il momento di adottare la stessa logica usata per le casse antirapina (es. cash-in/cash-out); limitare cioè l'accesso ai valori per mezzo di nuovi ed opportuni mezzi di riferma e speciali dispositivi.

Legare un segnale di correzione proveniente dai cassetti portasoldi non significa solo cassetto pieno o vuoto, ma consente di proporzionare anche i rischi assicurativi e ricreare quell'effetto di deterrenza che in questo momento è venuto a mancare.

Un'altra interessante soluzione tecnologica di sicurezza, perfettamente integrabile con quella suesposta, potrebbe essere il monitoraggio, attraverso centrale di telesorveglianza, dell'apertura e della chiusura dei mezzi forti "Bancomat" e non solo.

A tale scopo, sui battenti dei mezzi forti, dovrebbero essere installati dispositivi di riferma elettronico-meccanici di nuova generazione, controllabili e gestibili per mezzo di appositi sistemi informatizzati collegati con la stessa *CDT*. In questo modo tutte le serrature presenti nei mezzi forti diventerebbero altrettante periferiche della rete locale informatica presente in ogni agenzia bancaria. Sarebbe possibile così amministrare tutte le principali funzioni normalmente richieste per il controllo delle condizioni di accesso ad un mezzo di custodia, secondo moderni criteri di sicurezza e di operatività.

Ritengo che sia altresì necessario applicare all'impianto ATM ulteriori dispositivi di selezione e controllo degli operatori autorizzati ad aprire la cassaforte, mediante l'utilizzo di appositi badge e di codici PIN dinamici.

Con i succitati criteri innovativi, sarà possibile consentire a più utenti l'abilitazione all'uso della serratura; sarà altresì possibile attuare il ritardo di apertura da 1 a 99 minuti ed il blocco settimanale, secondo apposite fasce orarie; sarà inoltre consentito di programmare in anticipo le festività e l'ora legale dell'anno; attuare il blocco immediato della serratura, in caso di rapina; avviare il ritardo forzato della fascia oraria di chiusura, ecc. Tutti gli eventi e le operazioni suddetti potranno essere registrati su memoria elettronica, con indicazione di data e ora, della singola serratura interessata dall'evento, del codice identificativo dell'operatore addetto, ecc.

### **LE PROCEDURE DI GESTIONE E SICUREZZA**

Le aperture del mezzo di custodia dell'ATM per manutenzioni ordinarie e straordinarie e/o per quelle di emergenza (es. recupero tessere) dovrebbero sempre avvenire a seguito di sblocco del "sistema di riferma", da parte della centrale operativa di telesorveglianza e sotto controllo video "LIVE". I tecnici autorizzati alla manutenzione ed il personale incaricato dell'apertura dovrebbero essere identificati preventivamente dalla *CDT*, ad ogni singolo intervento.

Le suddette operazioni di manutenzione dovrebbero avvenire sempre in presenza di guardia giurata armata.

Per garantire un adeguata sicurezza al servizio di caricamento delle banconote sia svolto all'interno alla banca con proprio personale sia affidato a istituti specializzati,

occorrerebbe stabilire idonee procedure di sicurezza. Di seguito si forniscono alcuni suggerimenti in merito:

- Il caricamento dovrebbe avvenire a locali della banca chiusi (al mattino prima dell'apertura al pubblico, nell'intervallo di colazione, nel tardo pomeriggio);
- per impianti "*stand alone*" (locali "SELF" chiusi, supermercati, stazioni ed aeroporti, appositi spazi di ditte ecc.), gli addetti al servizio di trasporto e caricamento del contante dovrebbero fare allontanare, preventivamente, le persone estranee e, dopodiché, vigilare armati, con molta attenzione, durante tutto il tempo di svolgimento delle operazioni;
- l'operazione di apertura della cassaforte e di caricamento dovrebbe essere effettuata da almeno due addetti muniti, rispettivamente, di chiave e codice della serratura a combinazione, utilizzando il proprio badge e PIN di identificazione e tenendo pronto, all'occorrenza, un dispositivo tascabile di segnalazione allarme aggressione/rapina, ad onde radio;
- durante lo svolgimento delle suddette operazioni, la centrale di telesorveglianza dovrebbe tenere sotto costante controllo, anche mediante sistema di videosorveglianza, l'intera area in cui è installato l'impianto ATM;
- I codici numerici delle combinazioni dovrebbero essere sostituiti periodicamente;
- I mezzi di custodia dell'impianto ATM dovrebbero essere provvisti di "serrature a chiave cambiabile" affinché, oltre ai codici, anche le chiavi possano venire, periodicamente, sostituite.

In conclusione, occorre attuare un nuovo approccio che preveda una valutazione dei rischi che tenga in maggior conto quanto è emerso dai sinistri avvenuti di recente e che hanno coinvolto numerosi impianti "Bancomat". Le misure di prevenzione e protezione adottate dovranno pertanto essere commisurate alle mutate situazioni e non dovranno consentire ai criminali di impossessarsi con facilità del contenuto di tali impianti, neppure nei casi di infedeltà degli addetti. Un corretto monitoraggio dell'apertura delle riferme dei mezzi di custodia, l'identificazione e l'autorizzazione preventiva degli addetti al caricamento, l'applicazione di dispositivi di blocco delle serrature della cassaforte quando i cassetti sono ancora pieni, l'esistenza di idonee procedure di sicurezza e di audit ed un'attenta sorveglianza effettuata da centrale di telesorveglianza, sono gli elementi ormai indispensabili per evitare o quanto meno minimizzare i rischi di rapina e misteriosa sparizione del contante che incombono con sempre maggior frequenza su questi impianti.

1

## TIPOLOGIE DI ATTACCO AL "BANCOMAT"

OGNI ANNO SI VERIFICANO OLTRE 200 ATTACCHI (FURTI E RAPINE) A DANNO DEGLI IMPIANTI "BANCOMAT".

Le tipologie di attacco più comunemente attuate dai criminali sono:

- apertura forzata del battente mediante effrazione (attrezzi da scasso, gas ecc.), anche in presenza di impianto di allarme;
- rapina a mano armata, tenendo sotto minaccia il personale;
- misteriosa sparizione (?) mediante apertura con chiave (o simili) e codice della combinazione;
- asportazione dell'intero impianto (cassaforte) dalla sua sede, utilizzando un veicolo escavatore o altro mezzo di trasporto.

2

## LE CONSEGUENZE DI UN ATTACCO AL "BANCOMAT"

IL DANNO, IN TERMINI DI VALORI ASSICURATI NEGLI IMPIANTI ATM, PUO' ESSERE ANCHE RILEVANTE ED E' RAPPRESENTATO, SOSTANZIALMENTE, DALLE SEGUENTI VOCI:

- il crollo parziale delle strutture murarie del locale e/o dell'edificio;
- distruzione della componente hard-ware (inclusa cassaforte) dell'impianto "Bancomat";
- asportazione del denaro contante in esso contenuto.

.....E PER LA BANCA:

- temporanea messa fuori servizio dell'impianto, con conseguente disagio per la clientela;
- eventuali richieste di risarcimenti da terzi;
- perdita d'immagine.

3

## LA SITUAZIONE ATTUALE

NEGLI ULTIMI ANNI SI E' REGISTRATA NEL SETTORE BANCARIO UNA DIFFUSIONE SEMPRE MAGGIORE DELLE AREE "SELF SERVICE", CHE COMPREDONO ANCHE GLI IMPIANTI ATM.

LA CLIENTELA HA IN TAL MODO LA POSSIBILITA' DI UTILIZZARE I SERVIZI OFFERTI DALLA PROPRIA BANCA 24 ORE SU 24.

E' AUMENTATA PERTANTO LA DISPOSIBILITA' DI CONTANTE ALL'INTERNO DEGLI IMPIANTI "BANCOMAT" CHE, IN TAL MODO, DIVENTANO PIU' "APPETIBILI" PER LA CRIMINALITA' ORGANIZZATA.

CONSEGUENTEMENTE, E' AUMENTATA LA SINISTROSITA' (FURTI E RAPINE) IN TALI IMPIANTI.

4

## LA PROTEZIONE CONTRO L'EFFRAZIONE

è ancora oggi rappresentata essenzialmente da:

- miglioramento dell'ancoraggio dell'impianto "bancomat";
- irrobustimento della cassaforte (corpo e battente);
- rinforzo e protezione di riferme e serrature;
- installazione di dispositivi per rendere inefficace l'uso di gas e di altre miscele esplosive;
- applicazione di protezioni particolari antiripescaggio del contante;
- adozione di impianto di allarme antintrusione e antieffrazione localizzato (per segnalare tempestivamente l'inizio dell'attacco);
- presenza di sistema di videosorveglianza (come deterrente).

5

## LE PROTEZIONI ANTIRAPINA

Fino ad ora è stato possibile adottate le seguenti principali misure di prevenzione e protezione:

- ✓ serrature a tempo, ausiliarie, per ritardare l'apertura della cassaforte;
- ✓ dispositivi macchiatori delle banconote;
- ✓ videosorveglianza locale (con registrazione delle immagini).

.....Tuttavia, tali misure si sono rivelate insufficienti per evitare le rapine a danno degli impianti "bancomat"!

6

## LE PROTEZIONI ANTIRAPINA

Analizziamo brevemente quali tra le misure normalmente adottate per proteggere gli impianti ATM risultano insufficienti per arginare questa tipologia di evento criminoso:

➤ Il rinforzo meccanico della cassaforte:

Non ha rilevanza perché non vi è scasso.

➤ La serratura a tempo:

Utilizzabile soltanto per ATM installati in banca e gestiti direttamente da proprio personale. Tuttavia, in molti casi, i rapinatori attendono che trascorra il tempo di ritardo, tenendo sotto minaccia i dipendenti.

N.B. Il servizio esternalizzato non consente di attuare tempi di ritardo di apertura della cassaforte, per ovvie ragioni di costo.

➤ L'impianto d'allarme;

Se non gestito in tempo reale da CDT e soprattutto nel caso di attivazione e disattivazione locale, affidata agli operatori addetti, è da ritenersi insufficiente.

7

## LE PROTEZIONI ANTIRAPINA

.....e ancora:

➤ La videosorveglianza locale:

rappresenta un relativo deterrente; ha funzione di ricostruzione di evento, in caso di sinistro, ma se i rapinatori sono incensurati.....

➤ Le procedure di sicurezza:

La mancanza di procedure di sicurezza chiare, ben definite e di un accurato, periodico, *audit* interno, aumenta i rischi di furto e rapina legati a infedeltà e coercizione degli operatori addetti.

➤ I macchiatori del contante:

Inefficaci in caso di apertura senza scasso, mediante copie di chiavi e utilizzando i codici delle serrature a combinazione.

8

## IL PROBLEMA DELLE MISTERIOSE SPARIZIONI

E' un fenomeno in netta crescita. Dall'inizio dell'anno, sono oltre 80 i casi segnalati, con ingenti danni economici, ed i recenti fatti di cronaca lo confermano:



9

## IL PROBLEMA DELLE MISTERIOSE SPARIZIONI

Analoga problematica si è verificata, in precedenza, sugli impianti di trasferimento rapido del contante (es. casseforti tipo "GIANO", "ANY TIME", ecc.) in uso, prevalentemente, presso i supermercati.

Numerosi sono stati i danni di "misteriosa sparizione" !

In alcuni casi, a seguito di accurate perizie tecnico-assicurative, sarebbe emerso che si è trattato di infedeltà degli addetti al prelievo e trasporto valori. Infatti, la cassaforte sarebbe stata aperta, senza effrazione, con copia di chiavi ricavate dall'originale e utilizzo dell'esatto codice della serratura a combinazione.

10

## IL PROBLEMA DELLE MISTERIOSE SPARIZIONI

Nei casi di misteriosa sparizione avvenuti recentemente, gli impianti ATM sono stati vuotati durante il normale orario di lavoro delle agenzie, senza che sia stata attuata alcuna effrazione sul mezzo di custodia (?).....

Come ciò sia potuto accadere ha dell'incredibile. In tali casi, è stata dimostrata la totale inutilità delle misure di prevenzione e protezione adottate per proteggere questi impianti.

Ancora una volta, è dimostrato che l'anello più debole della catena della sicurezza è l'elemento umano!

11

## NUOVE SOLUZIONI CONTRO LA RAPINA E LE MISTERIOSE SPARIZIONI

### Quali miglioramenti occorre allora apportare alle attuali difese ?

Per rinforzi, blindature e ancoraggi non si può fare molto di più di quanto si è fatto finora.

Riguardo alle serrature, queste dovrebbero essere sostituite con altre di tipo elettronico-meccanico per poterne controllare l'apertura e la chiusura a distanza, mediante apposito sistema informatizzato di gestione, collegato con sala operativa di CDT.

Sarà necessario applicare all'impianto ATM dispositivi di selezione e controllo degli operatori autorizzati ad aprire la cassaforte, anche mediante l'utilizzo di codici dinamici.

12

## NUOVE SOLUZIONI CONTRO LA RAPINA E LE MISTERIOSE SPARIZIONI

Gli impianti d'allarme e di videosorveglianza dovranno essere gestiti anch'essi da sala operativa di *CDT*, secondo specifiche procedure di sicurezza, in conformità alla norma UNI 11068.

L'accesso all'area "SELF", l'attivazione e la disattivazione dell'impianto di allarme relativo al "Bancomat" dovranno avvenire sotto il diretto controllo dei sorveglianti della sala operativa della stessa *CDT*, previa identificazione dell'operatore autorizzato (badge + codice PIN) ed anche per mezzo di verifica delle immagini video, in modalità "LIVE".

Riguardo ancora alle procedure, sarà opportuno sempre verificare, a cura della *CDT*, il rispetto delle fasce orarie prestabilite per l'accesso ed il caricamento dell'ATM.

13

## **NUOVE SOLUZIONI CONTRO LA RAPINA E LE MISTERIOSE SPARIZIONI**

### Un'idea innovativa!

**Si potrebbe “legare” l’apertura del battente della cassaforte dell’ATM alla quantità di banconote contenute nei cassetti in essa presenti.**

14

### **Principio di funzionamento**

Il sistema dovrebbe prevedere l’installazione, all’interno del cassetto del bancomat, di un righello di sensori di posizione (reed-switch), posti in modo sequenziale.

Sullo spingibanconote verrebbe posizionato un puntatore magnetico che scorrerebbe solidale con esso e in ogni momento attiverrebbe uno dei suddetti “reed-switch” del righello.

La serie di “reed-switch” verrebbe collegata ad un microprocessore che in tal modo codificherebbe la posizione e la trasmetterebbe al suo ricevitore posto all’interno del bancomat.

Il ricevitore elaborerebbe le informazioni sullo stato di riempimento del cassetto.

L’informazione così elaborata potrebbe controllare inoltre il tempo di ritardo del dispositivo di apertura.

15

## LE PROCEDURE DI GESTIONE

Le aperture del mezzo di custodia dell'ATM per manutenzioni ordinarie e straordinarie e/o quelle di emergenza (es. recupero tessere) dovrebbero sempre avvenire a seguito di sblocco del "sistema di riferma", da parte della centrale operativa di telesorveglianza e sotto controllo video "LIVE".

I tecnici autorizzati alla manutenzione ed il personale incaricato dell'apertura dovrebbero essere identificati preventivamente dalla CDT, ad ogni singolo intervento.

Le operazioni di manutenzione dovrebbero avvenire sempre in presenza di guardia giurata armata.

16

## LE PROCEDURE DI GESTIONE

Devono essere predisposte adeguate procedure di sicurezza per il personale addetto al caricamento degli ATM, in particolare, quando il caricamento del contante viene esternalizzato. Tali procedure devono prevedere che:

- Il caricamento avvenga a locali della banca chiusi (al mattino prima dell'apertura al pubblico, nell'intervallo di colazione, nel tardo pomeriggio).
- Per impianti "*stand alone*" (locali "SELF" chiusi, supermercati, spazi aperti di ditte ecc.), gli addetti al servizio di trasporto e caricamento del contante devono fare allontanare, preventivamente, le persone estranee e vigilare armati, con molta attenzione, durante tutto il tempo delle operazioni.

17

## LE PROCEDURE DI GESTIONE

*....e ancora:*

- L'operazione di apertura della cassaforte e di caricamento dovrebbe essere effettuata da almeno due addetti muniti, rispettivamente, di chiave e codice della serratura a combinazione; utilizzando inoltre il proprio badge + PIN di identificazione e tenendo pronto, all'occorrenza, un dispositivo tascabile di segnalazione allarme aggressione, ad onde radio.
- Durante lo svolgimento delle suddette operazioni, la centrale di telesorveglianza dovrebbe tenere sotto costante controllo, anche mediante sistema di ripresa video, l'intera area in cui è installato l'impianto ATM.

18

## LE PROCEDURE DI GESTIONE

*....e infine:*

- I codici numerici delle combinazioni dovrebbero essere sostituiti periodicamente.
- I mezzi di custodia dell'impianto ATM dovrebbero essere provvisti di "serrature a chiave cambiabile" affinché, oltre ai codici, anche le chiavi possano venire periodicamente sostituite.