ABI

Apertura dei lavori

Convegno "Banche e Sicurezza"

Roma, 4-5 giugno 2015

Giovanni PIROVANO
Comitato Presidenza ABI

L'evoluzione della sicurezza

Il settore bancario dedica forte attenzione a mantenere elevati livelli di **fiducia nell'utilizzo dei propri servizi** attraverso investimenti in sicurezza informatica, sicurezza fisica, antifrode e per la continuità operativa:

- Le **Autorità di Vigilanza** sono attive nel far evolvere il contesto normativo adeguandolo alle nuove **necessità di utilizzo sicuro dei servizi bancari** anche da remoto
- La **cybersecurity** monitora costantemente l'**evoluzione degli attacchi** con l'obiettivo di **intercettare e contrastare** i tentativi di frode informatica
- Le **soluzioni di sicurezza** devono poter garantire un **presidio dinamico** al fine di conoscere e contrastare l'evoluzione dei fenomeni criminali e predisporre adeguate contromisure e attività di prevenzione
- La **sicurezza fisica** focalizza l'attenzione nella **riduzione delle attività predatorie** delle rapine e nell'identificazione di **nuove modalità di protezione** di filiali e ATM
- La **crescita dei pagamenti internet** richiede **nuove azioni di rafforzamento** nella gestione delle carte di pagamento

L'evoluzione normativa

La normativa di riferimento si modifica in relazione alla sicurezza informatica e dei pagamenti internet

- **Sicurezza degli accessi e dei servizi di pagamento**
  - Payment Service Directive II*
  - Raccomandazioni BCE in materia di sicurezza dei pagamenti internet (gennaio 2013)
  - Linee Guida EBA (dicembre 2014)
- **Valutazione del rischio informatico e correlazione con la gestione del rischio operativo**
  - Disposizioni di vigilanza prudenziale di Banca d'Italia in materia di sistema dei controlli interni, sistema informativo e continuità operativa - Circolare 263 (giugno 2013)
- **Sicurezza delle reti e delle informazioni**
  - Network and Information Security Directive*

* In via di emanazione

Evoluzione degli attacchi informatici

- Fenomeno in **continua evoluzione**, sia dal punto di vista tecnologico sia dal punto di vista del processo di attuazione
- **Tecniche avanzate di attacco:** social engineering, **malware sofisticati** o attacchi mirati a sfruttare **specifiche vulnerabilità**
- Necessario **monitorare costantemente** l'evoluzione del cybercrime e **anticipare la diffusione di nuovi malware** e tecniche di attacco
- Importante dotarsi di **strumentazione tecnologica adeguata**, proseguire le attività di **collaborazione**, persistere con le **iniziative di sensibilizzazione**

Clientela Corporate: **60%** degli attacchi durante la **sessione di log in del cliente** (attacchi man-in-the-browser o real time)

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, 2015, 25 rispondenti

Evoluzione delle contromisure

- Il settore bancario sta **contrastando** sempre di più il fenomeno del cybercrime
- Continuo **incremento nell'utilizzo dei servizi** di Internet Banking (nel 2014 registrati circa 1,2 miliardi di accessi al canale Internet)
- La percentuale di **clienti attivi che ha subito un danno economico** si è ridotta notevolmente:

Clientela Retail	clientela Corporate
1 caso di **perdita di denaro** ogni **1.700.000** accessi	**1** caso di **perdita di denaro** ogni **1.100.000** accessi

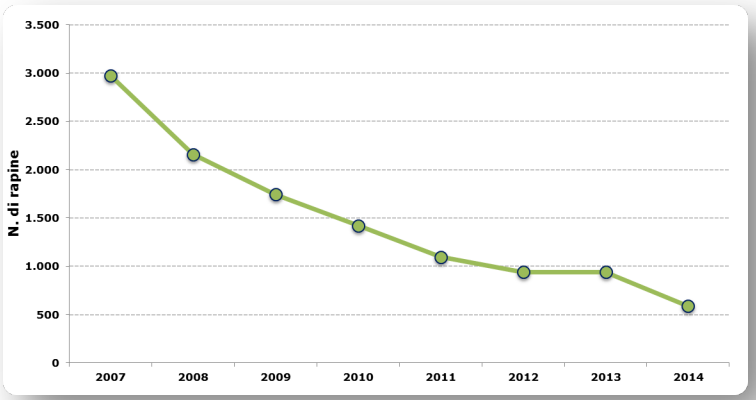
Contromisure notevolmente **efficaci:**
interrotti oltre il **97%** dei **tentativi** di frode nel 2014

- Non si deve distogliere il **livello di allerta** sul fenomeno
- **Obiettivi degli attacchi** sono i target di **clientela con maggiore disponibilità** (imprese) e quindi con **volumi economici** in gioco particolarmente elevati

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, 2015, 25 rispondenti

Sicurezza fisica: crollano le rapine

RAPINE IN BANCA *(2007-2014)*



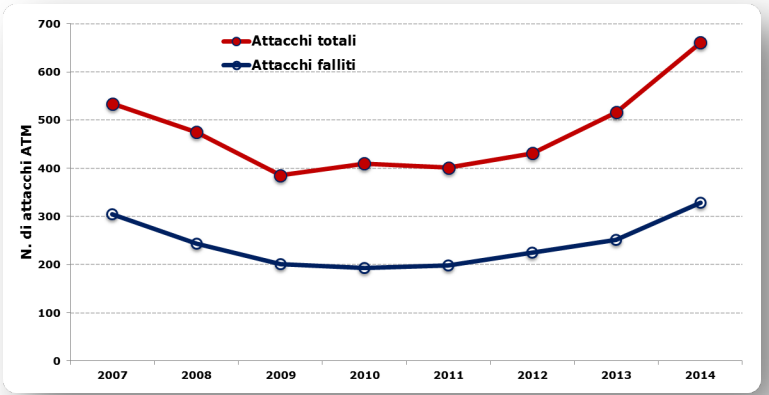
Fonte: elaborazioni su dati OSSIF

Variazione 2013-2014

-37,6% le rapine consumate

(da 941 a 587 rapine)

ATTACCHI AGLI ATM *(2007-2014)*



Fonte: elaborazioni su dati OSSIF

Variazione 2013-2014

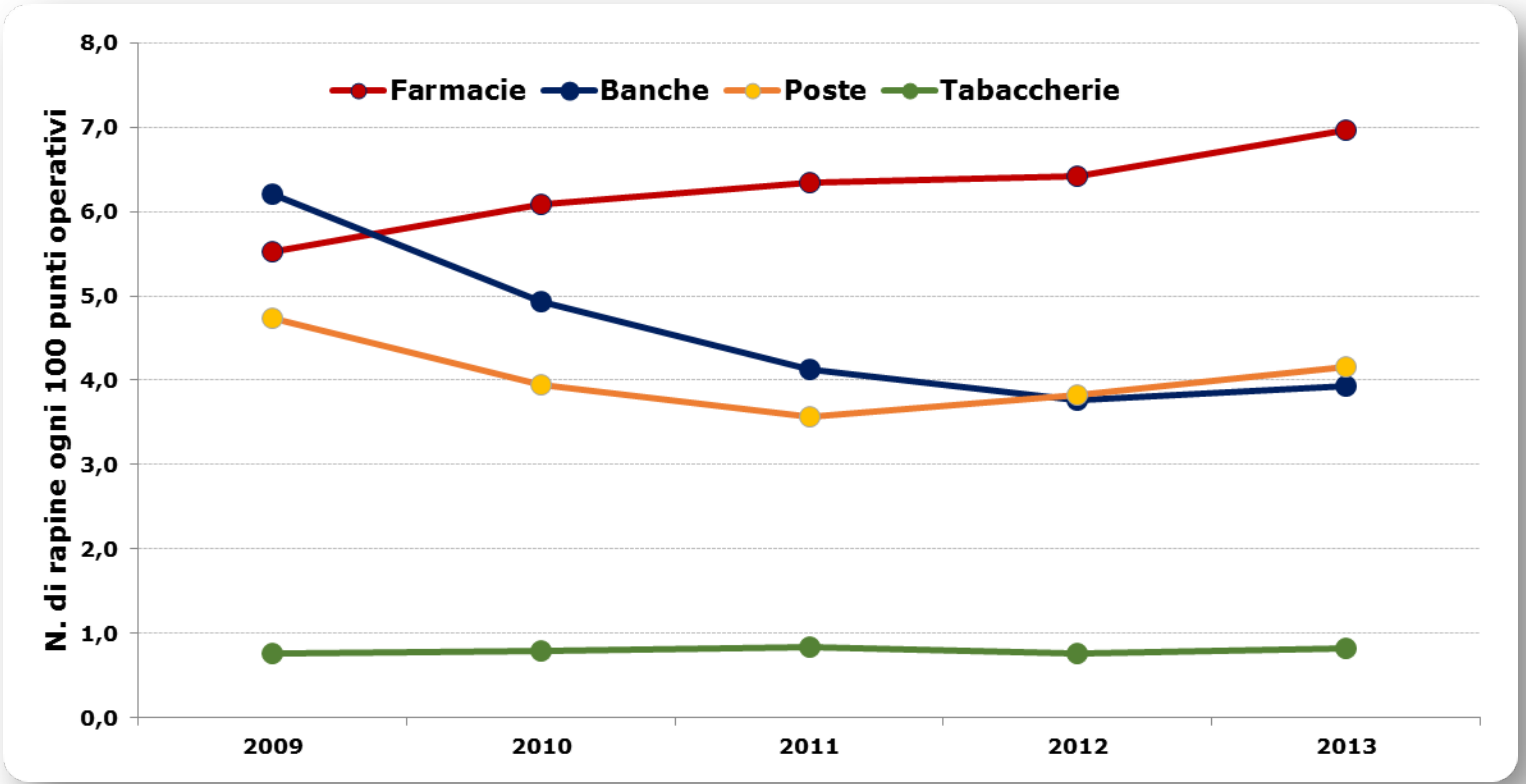
+28,1% gli attacchi agli ATM

(da 516 a 661)

La metà degli attacchi fallisce

Sicurezza fisica: Osservatorio intersettoriale

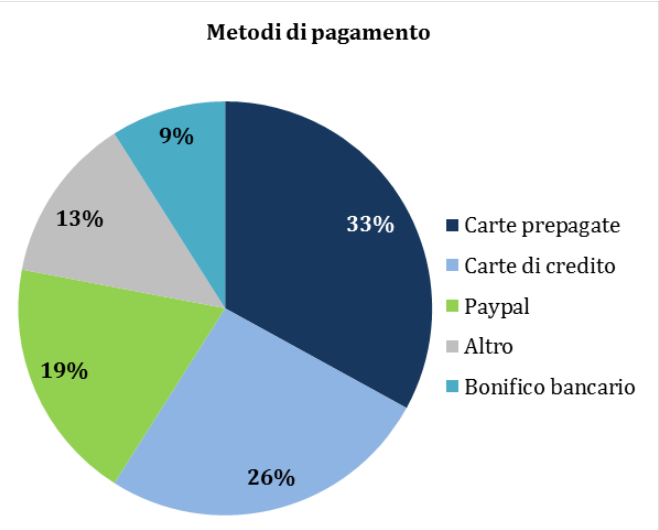
RAPINE OGNI 100 PUNTI OPERATIVI PER SETTORE



Fonte: Elaborazioni OSSIF su dati Ministero dell'Interno

La situazione attuale in Italia per l'e-commerce

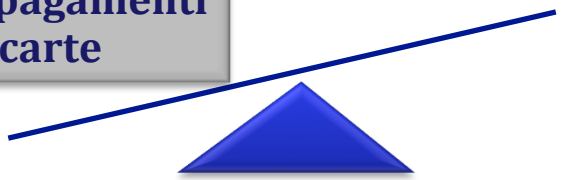
- **34%** circa degli internet user effettua anche **acquisti online**
- Su 10 Mln di e-shopper, circa il **75%** di individui effettua anche **pagamenti online** utilizzando canali differenziati
- Nel 2013, il **55,2%** del numero di **transazioni** sono state **disconosciute** con causale «utilizzo fraudolento su internet» (+97,1% rispetto al 2012)



Frodi su pagamenti con bonifici

Frodi su pagamenti con wallet

Frodi su pagamenti con carte



- **Identity theft**
- **Fenomeni di malwering (pharming, phishing, spear phishing, hidden page…)**
- **Arp poisoning**
- **Key logging**
- **Firesheep**

Profili di sicurezza dei pagamenti online

Strategie di contrasto alle frodi sui pagamenti via internet

- Per evitare la duplicazione / replica dei dati, si favorisce l'**utilizzo di dati dinamici** e **«one time»**.
- Per elevare il grado di confidenzialità, si ricorre al **rafforzamento dei processi di autenticazione** fra soggetti/ sistemi interagenti con l'utilizzo di diverse tipologie di certificati.
- Per elevare il grado di protezione dei dati si ricorre alla **segregazione delle reti**.

Flusso di pagamento standard

Pagamento standard su web

Richiede, al momento dell'acquisto, l'inserimento di alcuni dati riportati sulla carta: PAN della carta Titolare; Data scadenza Altri dati sulla carta: CVC, CVC2, etc.

Flusso di pagamento con strong authenti-cation

Pagamento con 3D secure

- L'utente si registra al servizio e sceglie una password e un messaggio personale
- Al momento del pagamento, inserisce i dati della carta
- I siti web protetti da 3d secure vengono identificati in modo esplicito
- L'utente inserisce la password scelta in precedenza
- Conferma e fine dell'acquisto

All'interno del convegno

- L'evento vuole **analizzare e approfondire i presidi di sicurezza** maggiormente coinvolti all'interno del settore bancario

Giorno 1: mattina - Sessioni plenarie

- *La sicurezza nelle banche italiane: uno scenario che cambia*
- *Le nuove sfide del cybercrime*

Giorno 1: pomeriggio - Sessioni parallele

- *SICUREZZA FISICA: Difendiamo insieme il territorio*
- *SICUREZZA INFORMATICA: Pronti al cyber attacco?*
- *FRODI: Contrastare le frodi di nuova generazione*

Giorno 2: mattina - Sessioni parallele

- *SICUREZZA FISICA: Norme, strumenti e soluzioni per la prevenzione*
- *SICUREZZA INFORMATICA: Standard, compliance e gestione dei rischi*
- *FRODI: Cyber Intelligence e dati sulle frodi*

Giorno 2: pomeriggio

- *WORKSHOP "LA SICUREZZA PER LE IMPRESE"*