PROTOCOLLO DI INTESA

PER LA PREVENZIONE DELLA

CRIMINALITÀ AI DANNI DELLE BANCHE E

DELLA CLIENTELA

La Prefettura, l'ABI e le banche firmatarie del *Protocollo d'intesa per la prevenzione della criminalità ai danni delle banche* (di seguito "Protocollo"),

CONSIDERATO

- che la domanda di sicurezza investe il settore bancario, esposto agli attacchi della criminalità comune e organizzata;

- che alle Forze dell'ordine spetta istituzionalmente la difesa del cittadino;

- che la necessità di proteggere le dipendenze bancarie è un preciso impegno delle banche nei confronti dei dipendenti e della clientela e risponde all'esigenza di consentire l'operatività in condizioni di sicurezza;

- che l'azione della criminalità contro le dipendenze bancarie evolve grazie alle potenzialità delle nuove tecnologie: in particolare, come dimostra l'emergere di attacchi con tecniche di *cyber physical security*, cioè attacchi multivettoriali in cui vengono usate congiuntamente tecniche di violazione fisica, informatica e di social engineering;

PRESO ATTO

- della proficua collaborazione tra Prefetture, Forze dell'ordine, ABI e banche per contrastare la criminalità ai danni delle banche;

- dei contenuti del Protocollo d'intesa tra l'ABI e il Dipartimento di Pubblica sicurezza del Ministero dell'Interno sottoscritto il 14 maggio 2018;

CONVENGONO QUANTO SEGUE

Art. 1 – Informazioni di carattere generale

Le banche si impegnano, possibilmente entro un termine di 25 giorni dalla sottoscrizione, a inserire sul Portale www.ossif.it le seguenti informazioni:

- il nome, il numero telefonico e la e-mail del responsabile o della struttura alla quale è possibile rivolgersi per le problematiche di sicurezza di carattere generale;
- il nome e il numero telefonico di un referente per le problematiche concernenti le singole dipendenze o, in alternativa al secondo, un recapito telefonico facente capo ad una centrale operativa della banca a cui far riferimento nelle 24 ore;
- l'elenco delle dipendenze, i relativi indirizzi, i numeri telefonici e di fax;
- l'orario di apertura al pubblico antimeridiana e pomeridiana, dal lunedì al venerdì, e di apertura eventuale nelle giornate di sabato e domenica.

OSSIF, il Centro di Ricerca dell'ABI sulla sicurezza anticrimine, provvederà a trasmettere le suddette informazioni alla Prefettura.

Art. 2 – Segnalazione di situazioni di rischio

Le banche si impegnano a segnalare alle Forze dell'ordine ai numeri telefonici indicati nell'unito prospetto:

- carenze gravi e imprevedibili delle misure di sicurezza (es. guasto dei sistemi relativi al controllo degli accessi);
- movimenti sospetti di persone all'interno e all'esterno delle dipendenze bancarie;
- eccezionali aggravamenti del rischio (es. aumento anomalo giacenze di cassa);
- lavori da svolgere durante l'orario di apertura della dipendenza che inficino l'efficacia delle misure di sicurezza (es. sostituzione di un sistema di allarme);
- altre situazioni particolari di rischio in cui versano le dipendenze bancarie.

Art. 3 – Valutazione dei Rischi

La valutazione dei rischi che possono riguardare il personale, la clientela e i beni aziendali deve considerare eventi come le rapine, i furti ai danni delle apparrecchiature ATM, gli attacchi multivettoriali (cyber physical security), le truffe alla clientela, gli atti vandalici e terroristici, le aggressioni al personale non a scopo predatorio. [1]

La probabilità di accadimento degli eventi "rapina" e "furto ATM" (e la conseguente valutazione del rischio delle dipendenze) può essere quantificato solo in misura limitata, in quanto condizionata da molteplici fattori che, da un lato, esulano dallo spazio di intervento delle banche (fattori esogeni), dall'altro seguono dinamiche non prevedibili e non riconducibili a modelli previsionali definiti.

Ciò nonostante, le banche si impegnano a valutare il rischio rapina di ciascuna dipendenza e il rischio di furto alle apparecchiature ATM aggiornando periodicamente detta valutazione, in relazione all'evoluzione dei fenomeni criminosi e alle eventuali informazioni fornite dalle Forze dell'ordine.

In questa prospettiva, le banche si impegnano altresì ad utilizzare strumenti di analisi territoriale predisposti in collaborazione con OSSIF e/o condivisi con lo stesso Osservatorio per determinare le aree a maggior rischio (es. Geocrime Analyst).

La probabilità di accadimento degli "atti vandalici e terroristici" può essere considerata solo in misura qualitativa e non può essere riferita puntualmente alle singole dipendenze. La sua valutazione pertanto si basa: sull'analisi delle fonti pubbliche prodotte dalle deputate Istituzioni dello Stato, sugli eventuali incontri promossi periodicamente tra le Forze dell'Ordine e le banche, su analisi in materia realizzate da qualificate Associazioni esterne; sulla condivisione di informazioni tra le banche.

[1] Per "aggressioni al personale non a scopo predatorio" si intendono azioni quali, ad esempio, minacce e atti di aggressione fisica praticati sul luogo di lavoro da soggetti esterni all'organizzazione tali da mettere a repentaglio la salute o la sicurezza del personale dipendente.

Analogamente, la probabilità di accadimento delle "aggressioni al personale non a scopo predatorio" può essere considerata solo in misura qualitativa e non puntuale, in quanto si tratta di azioni soggettive non prevedibili, spesso condotte senza motivazioni apparenti.

Art. 4 – Misure di sicurezza a mitigazione delle rapine

Le banche si impegnano a comunicare le notizie sulle rapine ai danni delle proprie dipendenze inserendo nel Data-Base Anticrimine di OSSIF le relative informazioni di dettaglio nei giorni successivi al verificarsi dell'evento criminoso.

Le banche si impegnano a dotare ciascuna dipendenza - entro tre mesi dalla data di sottoscrizione - di almeno 5 misure di sicurezza, di cui obbligatoriamente la videoregistrazione e il dispositivo di custodia valori ad apertura ritardata o il dispositivo di erogazione temporizzata del denaro[2]. Le altre 3 misure devono essere individuate tra quelle di seguito elencate:

1. bussola
2. metal detector
3. rilevatore biometrico
4. vigilanza
5. videocollegamento/videosorveglianza
6. videoregistrazione
7. sistema anticamuffamento
8. allarme antirapina
9. sistema di protezione perimetrale attiva/passiva
10. bancone blindato/area blindata ad alta sicurezza
11. dispositivo di custodia valori ad apertura ritardata
12. dispositivo di erogazione temporizzata del denaro
13. gestione centralizzata dei mezzi forti

[2] L'impegno di adottare il dispositivo di erogazione temporizzata del denaro non si applica alle dipendenze sprovviste di casse – ad esempio dipendenze con solo macchine self service gestite da personale della banca

14. sistema di macchiatura delle banconote
15. sistema di tracciabilità delle banconote
16 procedure comportamentali codificate per operare in sicurezza[3]
17 formazione anticrimine.

Con riferimento alla videoregistrazione, le banche si impegnano, per le nuove istallazioni e per l'adeguamento delle preesistenti, ad utilizzare la tecnologia digitale, che gradualmente sostituirà quella analogica.

Ferme restando le misure minime concordate, ogni banca si impegna a selezionare sia quantitativamente sia qualitativamente i sistemi di difesa più opportuni in funzione della valutazione del rischio della singola dipendenza.

In caso di recrudescenza delle rapine in specifica dipendenza – caratterizzata da almeno tre rapine nell'arco di vigenza del presente Protocollo d'intesa (2 anni) – le banche si impegnano ad adottare quale intervento di mitigazione una misura aggiuntiva a quelle minime stabilite nell'art. 4.

Sono escluse le dipendenze in cui il personale non lavora contante[4].

Art. 5 – Misure di sicurezza a mitigazione dei furti agli ATM

Le banche si impegnano a comunicare le notizie sulle rapine e sui furti subiti ai danni delle proprie apparecchiature ATM inserendo nel Data-Base Anticrimine di OSSIF le

[3] Le procedure comportamentali si intendono adeguate ai fini del presente Protocollo se: (a) sono codificate per iscritto, (b) vengono diramate a tutte le filiali, (c) sono periodicamente aggiornate rispetto all'evoluzione dei modelli distributivi e delle soluzioni di sicurezza della banca, (d) individuano responsabilità e modalità operative almeno per i seguenti ambiti: apertura della filiale, gestione degli ingressi del pubblico, controllo dei fornitori in filiale, custodia delle chiavi della filiale, custodia delle chiavi dei mezzi forti, cautele per lavorare il contante in sicurezza, cautele per lo scambio di valori con istituti specializzati, limiti di contante detenibile nelle casse, limiti di contante detenibile negli ATM (con o senza riciclo), comportamenti da tenere in caso di rapina, cautele per la gestione di informazioni sensibili per la sicurezza, controlli sullo stato delle misure di protezione realizzabili dai dipendenti di filiale.

[4] Ad esempio: dipendenze dedicate solo alla consulenza; dipendenze senza casse e con macchine self service gestite da operatori esterni specializzati; punti informativi; ecc..

relative informazioni di dettaglio nei giorni successivi al verificarsi dell'evento criminoso.

Compatibilmente con la rischiosità delle singole installazioni, le banche si impegnano a proteggere le proprie apparecchiature ATM, dotandole, entro sei mesi dalla data di sottoscrizione, di almeno tre sistemi di sicurezza tra quelli di seguito elencati:

1. protezione con impianto di allarme locale e/o remoto connesso a sensori antiscasso/antintrusione
2. blindatura del mezzo forte
3. rinforzo aggiuntivo della vetrina ove è installata l'apperecchiatura ATM o dello spazio antistante con difese passive quali putrelle, archetti, dissuasori atti ad impedire l'asportazione del mezzo forte
4. sensori per la presenza di gas e/o dispositivi atti a impedire l'esplosione
5. sistemi per localizzare e/o tracciare le banconote rubate e/o dispositivi per rendere inutilizzabili le banconote rubate
6. dispositivi per localizzare/rintracciare gli ATM asportati
7. dispositivi attivi per proteggere il locale contenente il mezzo forte e/o la vetrina ove è installato il mezzo forte
8. dispositivi atti ad impedire l'introduzione di esplosivo liquido, solido o gassoso nel mezzo forte
9. misure hardware e/o software per la protezione delle componenti per l'interazione con la carta
10. collocazione del mezzo forte in area blindata ad alta sicurezza
11. dispositivi passivi per rafforzare la blindatura e l'ancoraggio del mezzo forte (cd gabbie esterne)
12. videoregistrazione
13. sistemi predittivi di analisi
14. rinforzo dei dispositivi di riferma.

In caso di recrudescenza degli attacchi ai danni di una specifica apparecchiatura ATM – caratterizzata da almeno tre attacchi nell'arco di vigenza del presente Protocollo d'intesa (2 anni) – le banche si impegnano ad adottare su tale apparecchiatura, quale intervento di mitigazione, una misura aggiuntiva a quelle minime stabilite nell'art. 5.

Gli ATM collocati presso terzi non rientrano nel presente Accordo in quanto si avvalgono anche dei dispositivi di sicurezza adottati dalla proprietà[5].

Art. 6 – Prevenzione dei rischi multivettoriali *(cyber physical security)*

Le banche si impegnano a prevenire gli attacchi multivettoriali realizzati con tecniche di *cyber physical security* a danno delle dipendenze bancarie, che integrano le tecniche di violazione di tipo fisico con quelle di tipo informatico e di ingegneria sociale.

In particolare le banche si impegnano a censire gli attacchi realizzati ai danni delle dipendenze bancarie con le nuove tecniche di *cyber physical security*. OSSIF provvederà ad acquisire i dati presso le diverse fonti di raccolta per effettuare analisi che verranno messe a disposizione delle Forze dell'Ordine.

Inoltre OSSIF si impegna ad attivare specifiche iniziative per monitorare la diffusione degli attacchi "multivettoriali", promuovere la creazione e la condivisione di metodologie di prevenzione e mitigazione, stimolare lo sviluppo della cultura della *cyber physical security*.

Art. 7 – Prevenzione delle truffe

Le banche si impegnano a contribuire alla prevenzione delle truffe ai danni della popolazione di età più avanzata, ovvero con educazione finanziaria contenuta.

[5] Ad esempio: ATM presso caserme, comuni, ospedali, centri commerciali, ecc.

Le attività di prevenzione potranno riguardare:

- consigli generali per evitare l'esposizione al rischio truffe;
- numeri di soccorso utili per reazione immediata;
- un attento monitoraggio delle truffe al fine di individuare le buone pratiche da condividere ed estendere nei diversi ambiti territoriali.

Art. 8 - Prevenzione degli attacchi vandalici e terroristici

Le banche si impegnano a censire le notizie relative agli atti vandalici e terroristici ai danni delle proprie dipendenze. OSSIF provvederà ad acquisire i dati presso le diverse fonti di raccolta per effettuare analisi che verranno messe a disposizione delle Forze dell'Ordine.

Le banche si impegnano altresì ad informare e/o formare il proprio personale sulle cautele da adottare.

Art. 9 - Prevenzione delle aggressioni al personale non a scopo predatorio

Le banche si impegnano a censire gli atti di aggressione al personale delle proprie dipendenze, non inerenti alla commissione di reati a scopo predatorio (quali le rapine).

Le banche si impegnano altresì ad informare e/o formare il proprio personale sulle cautele da adottare.

Art. 10 – Mappatura dei sistemi di videosorveglianza

Le banche si impegnano a segnalare nel Data-Base Anticrimine di OSSIF tutti gli apparati di videosorveglianza presenti all'esterno delle proprie dipendenze.

Ciò al fine di soddisfare eventuali richieste delle Prefetture in merito al censimento, alla mappatura e alla georeferenziazione di tutti gli apparati di videosorveglianza installati in luoghi pubblici o aperti al pubblico, ad opera di Enti pubblici o privati. In questo modo le Forze dell'ordine saranno in grado di conoscere la presenza e la disponibilità di fonti multimediali in una determinata area di interesse con evidenti benefici nell'azione di prevenzione e investigativa.

Tutto ciò anche nell'ambito dell'attuazione delle linee-guida diramate dal Ministero dell'Interno il 30 aprile 2015.

Art. 11 – Comunicazione delle misure di sicurezza

Le banche per aumentare la deterrenza delle misure di sicurezza devono adottare, ove ritenuto necessario, strumenti di comunicazione (vetrofanie o similari) che pubblicizzino alcune delle soluzioni di sicurezza presenti nelle proprie dipendenze.

Allo scopo può essere utilizzata, ad esempio, la "messaggistica di sicurezza" predisposta da OSSIF, il Centro di Ricerca dell'ABI sulla sicurezza anticrimine."

Art. 12 – Esigenze di privacy

Le banche si impegnano a dare piena e completa applicazione alle previsioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

Per quanto riguarda i sistemi di videoregistrazione, i trattamenti di dati personali dovranno essere effettuati altresì rispettando le misure e gli accorgimenti prescritti dal Garante per la protezione dei dati personali ("Provvedimento in materia di videosorveglianza – 8 aprile 2010").

Dovrà essere, altresì, assicurata l'osservanza delle prescrizioni emanate dal Garante, nel Provvedimento del 27 ottobre 2005, in caso di ricorso al dispositivo del rilevatore biometrico.

L'utilizzo dei sistemi di videoregistrazione, inoltre, dovrà tener conto della indicazioni contenute nella circolare del Ministero dell'Interno n.558/1/421.2/70/456 datata 8 febbraio 2005.

Le banche, nell'adempiere alla normativa generale vigente in materia di protezione dei dati personali, confermano altresì che le apparecchiature che consentono la registrazione visiva degli ambienti, destinati al pubblico e allo svolgimento del lavoro, sono state istallate e continueranno ad essere adottate e utilizzate nel rispetto di quanto previsto dall'art. 4 della Legge 20 maggio 1970 n. 300.

Art. 13 – Manutenzione delle misure di sicurezza

Le banche si impegnano ad attuare, almeno su base annua e per tutti i dispositivi di sicurezza che lo richiedano, le attività di verifica e/o manutenzione preventiva atte a consentirne il miglior funzionamento.

Le banche si impegnano altresì ad assicurare in tempi brevi il ripristino di impianti di sicurezza che hanno subito guasti.

Art. 14 – Informazione

Le banche si impegnano ad intensificare, nei confronti dei propri dipendenti, le attività di informazione inerenti la sicurezza anticrimine, anche tramite specifica normativa (ad es. la Guida ABI sull'antirapina per il personale di sportello, i contenuti info/formativi del Centro Antifrode di BANCOMAT SpA) al fine di individuare standard comportamentali adeguati alle specifiche circostanze.

Art. 15 – Ruolo della Prefettura

La Prefettura promuove Riunioni di coordinamento delle Forze di Polizia o Comitati Provinciali per l'Ordine e la Sicurezza Pubblica per la trattazione di problematiche inerenti la sicurezza bancaria, anche a seguito di situazioni di particolare criticità che dovessero essere segnalate dalle Forze di Polizia e/o dalle parti del presente protocollo ovvero dalle Organizzazioni Sindacali di categoria.

Art. 16 – Ruolo delle Forze dell'ordine

Le Forze dell'ordine si impegnano nei confronti delle banche a:

- segnalare, anche per il tramite di OSSIF, eventuali fattori di rischio che possano tradursi in eventi criminosi;
- intervenire, su richiesta delle banche e a fronte di reali stati di necessità, a specifici incontri con le banche stesse per fornire informazioni in materia di sicurezza anticrimine
- partecipare a workshop organizzati da OSSIF per promuovere presso le banche la cultura della sicurezza anticrimine, *della cyber physical security*, della prevenzione delle truffe alla clientela, degli atti vandalici e terroristici, nonché delle aggressioni al personale non a scopo predatorio.
- condividere linee-guida per la prevenzione e il contrasto della criminalità.

Art. 17 – Ruolo dell'ABI

L'ABI si impegna a fornire, attraverso OSSIF, una sintesi delle informazioni contenute nel data-base di settore ai fini delle valutazioni sullo specifico ambito.

Art. 18 – Durata

Il Protocollo che le parti sottoscrivono, ciascuna per quanto di competenza, in relazione agli impegni espressamente indicati, avrà la durata di 24 (ventiquattro) mesi a decorrere dalla data odierna e sarà tacitamente rinnovato a scadenza salvo diverse intese tra le parti.

Allegati

Allegato 1

REFERENTI FORZE DELL'ORDINE

Il presente allegato sarà predisposto dalla Prefettura

Allegato 2

FIRMATARI

Il presente allegato sarà predisposto dall'ABI