Convergenza tra sicurezza fisica, logica e antifrode: analisi dei principali scenari di compromissione dei dispositivi ATM e degli strumenti tecnologici in dotazione a Poste Italiane S.p.A

Indice

Executive Summary

Questo studio sviluppa un'analisi dei principali scenari di compromissione della sicurezza fisica e logica dei dispositivi ATM estendendo tuttavia la trattazione anche ad altri strumenti tecnologici in dotazione a Poste Italiane, a supporto di transazioni bancarie o similari. La descrizione prende in considerazione i diversi fenomeni di frode o attacco a partire da un contesto generale illustrando metodologie di attacco e principali contromisure adottabili e, ove applicabile, è presente la contestualizzazione alla realtà aziendale di Poste Italiane in termini di stato dell'arte e iniziative future volte a contrastare al meglio le evoluzioni prevedibili negli scenari di attacco.

Tra i principali punti di riflessione, vengono messi in luce:

- il trend crescente di attacchi legati alla clonazione della carta a banda magnetica e all'intercettazione del PIN trova un riscontro diretto nell'aumento riscontrabile delle manomissione dei terminali in termini di alterazione della tastiera, applicazione di sistemi di videoripresa, sistemi di intercettazione e compromissione del lettore di carte magnetiche;
- l'impatto sempre più grave degli attacchi tramite esplosione del terminale ATM e conseguente ingresso nella sede per la sottrazione del denaro. Elemento di primaria importanza, in questo senso, è dato dalla costatazione del fatto che l'entità del danno alle infrastrutture e all'operatività della sede è di gran lunga superiore a quella direttamente connessa ai valori prelevati;
- la diffusione delle rapine durante il caricamento dei terminali ATM. Sebbene la casistica mostri un andamento stabile, il fenomeno rimane diffuso e l'importo ingente del totale dei danni giustifica lo sviluppo di iniziative di contrasto.

Nel contesto di Poste Italiane l'analisi sviluppata nel documento ha evidenziato altri spunti di interesse tra cui:

- la transizione attualmente in atto verso una rete di terminali completamente compatibile con la tecnologia basata su chip, non solo può contrastare tipologie di compromissione prettamente fisiche basate sull'alterazione dei lettori o delle tastiere, ma contribuisce a rafforzare la sicurezza logica dell'architettura aumentando la sicurezza nella gestione delle informazioni (in particolare le credenziali dell'utente e la loro verifica);
- per quanto riguarda le violazioni di natura logica (intrusione nel pc dell'ATM, alterazione del canale di comunicazione di rete), queste non comportano ancora impatti comparabili a quelli citati in precedenza per gli attacchi fisici. Tuttavia, la progressiva introduzione di diverse tipologie di terminali sul campo e la crescente interconnessione tra la rete Postamat e altri servizi erogabili per via telematica giustifica un alto livello di attenzione;
- attività di analisi interne hanno messo in luce alcune debolezze, note in ambito aziendale, relativamente a processi strettamente connessi con la gestione operativa dei terminali ATM, in particolare per quanto riguarda la creazione del legame con il sistema di gestione centrale e i processi di analisi e tracciatura delle anomalie.

Sono quindi state presentate, mediante l'identificazione di elementi di interesse molto contestualizzati alla realtà aziendale, casistiche di illeciti o frode che, seppure non direttamente collegate ai terminali ATM e

meno frequenti, preludono o lasciano modo di temere scenari futuri di diffusione ed è pertanto utile che vengano portate all'attenzione. Tra i terminali oggetto di violazioni di questo tipo sono stati considerati:

- i chioschi self-service (totem);
- i terminali operatore (le Postazioni di Lavoro);
- in parte, i terminali ATM evoluti.

Infine, dalle considerazioni specifiche proposte nel documento, relativamente a Poste Italiane per i vari temi affrontati, possono emergere alcune considerazioni generali:

- un'elevata attenzione dell'azienda verso la tutela della sicurezza fisica dei terminali ATM e della sicurezza perimetrale degli stessi e delle sedi. I fenomeni che al momento destano maggiore preoccupazione sono ben noti in azienda ed esistono passi concreti per l'adozione di contromisure puntuali e per il costante monitoraggio delle evoluzioni nelle tecnologie di contrasto;
- la decisa volontà di tutelare la sicurezza delle credenziali degli utenti, mediante la messa in atto di meccanismi di prevenzione al fine di evitare la loro sottrazione;
- una forte formalizzazione dei processi di predisposizione e gestione dei terminali, sebbene esistono aree non completamente sottoposte a procedure condivise, per i quali sussistono alcune debolezze di processo (e non conformità rispetto agli standard di riferimento) di cui l'azienda è ben consapevole;
- la possibilità di introdurre un rafforzamento tecnologico relativamente alla tematica della protezione interna dell'infrastruttura di interconnessione specifica per la rete ATM.