

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

4

1 INTRODUZIONE

ERRORE. IL SEGNALIBRO NON È DEFINITO.

1.1 La metodologia descrittiva

Errore. Il segnalibro non è definito.

1.2 La fenomenologia analizzata

Errore. Il segnalibro non è definito.

1.2.1 Truffe elettroniche

Errore. Il segnalibro non è definito.

1.2.2 Attacchi alla cassaforte

Errore. Il segnalibro non è definito.

1.2.3 Una panoramica su Poste Italiane

Errore. Il segnalibro non è definito.

2 PANORAMICA SUGLI SPORTELLI ATM E SU POSTAZIONI SIMILI

ERRORE. IL

SEGNALIBRO NON È DEFINITO.

2.1 Finalità dei dispositivi ATM

Errore. Il segnalibro non è definito.

2.1.1 Nota sulla generica interazione tra utente e terminale

Errore. Il segnalibro non è definito.

2.1.2 Prelievo/versamento di contante o altri valori

Errore. Il segnalibro non è definito.

2.1.3 Fruizione servizi e disposizione pagamenti

Errore. Il segnalibro non è definito.

2.1.4 Consultazioni

Errore. Il segnalibro non è definito.

2.2 Tipologie dei dispositivi e delle postazioni

Errore. Il segnalibro non è definito.

2.2.1 ATM tradizionali

Errore. Il segnalibro non è definito.

2.2.2 Cassa continua

Errore. Il segnalibro non è definito.

2.2.3 ATM “evoluti”

Errore. Il segnalibro non è definito.

2.2.4 Chioschi multimediali self-service (“Totem”)

Errore. Il segnalibro non è definito.

2.2.5 POS interni (Postazioni operatore)

Errore. Il segnalibro non è definito.

3 LA SICUREZZA FISICA DEI DISPOSITIVI ATM

ERRORE. IL SEGNALIBRO NON È

DEFINITO.

3.1 Livelli di certificazione

Errore. Il segnalibro non è definito.

3.2 Panoramica sulle principali tipologie di compromissione fisica degli apparati ATM

Errore. Il segnalibro non è definito.

3.2.1 Sottrazione/clonazione carta

Errore. Il segnalibro non è definito.

3.2.2 Esplosione

Errore. Il segnalibro non è definito.

3.2.3 Rapine durante la fase di caricamento dell’ATM

Errore. Il segnalibro non è definito.

3.2.4 Attacchi portati dall’interno della sede

Errore. Il segnalibro non è definito.

3.2.5 Rimozione del terminale

Errore. Il segnalibro non è definito.

3.2.6 Alterazione dell’emettitore di banconote

Errore. Il segnalibro non è definito.

3.2.7 Attacchi mediante scariche o impulsi elettrici

Errore. Il segnalibro non è definito.

4 LA SICUREZZA LOGICA NEI DISPOSITIVI ATM ERRORE. IL SEGNALIBRO NON È DEFINITO.

4.1 Principali standard di riferimento

Errore. Il segnalibro non è definito.

4.1.1 PCI-DSS

Errore. Il segnalibro non è definito.

4.1.2 PCI-PIN

Errore. Il segnalibro non è definito.

4.1.3 PA-DSS

Errore. Il segnalibro non è definito.

4.1.4 Documentazione SPE-DEF di CoGeBan

Errore. Il segnalibro non è definito.

4.2 Panoramica sulle principali tipologie di compromissione logica degli apparati ATM Errore. Il segnalibro non è definito.

4.2.1 Autenticazione

Errore. Il segnalibro non è definito.

4.2.2 Tracciamento delle operazioni

Errore. Il segnalibro non è definito.

4.2.3 Installazione, hardening e configurazione del software

Errore. Il segnalibro non è definito.

4.2.4 Connessione al gestore centrale

Errore. Il segnalibro non è definito.

4.2.5 Accessi per manutenzione

Errore. Il segnalibro non è definito.

5 ALTRE TIPOLOGIE DI ILLECITO DI INTERESSE ERRORE. IL SEGNALIBRO NON È DEFINITO.

5.1.1 POS per operatori

Errore. Il segnalibro non è definito.

5.1.2 Totem non presidiati

Errore. Il segnalibro non è definito.

5.1.3 Gestione delle problematiche legate al versamento di denaro falso nei terminali “evoluti”

Errore. Il segnalibro non è definito.

Errore. Il

6 CONSIDERAZIONI FINALI SULLO SCENARIO “POSTE ITALIANE” ERRORE. IL SEGNALIBRO NON È DEFINITO.

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 manomissioni 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 constatazione 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, precludono 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.