ATM E SICUREZZA

LE NUOVE FRONTIERE DELLA CYBERSECURITY

OPINION PAPER

THE # NEXTGENBANK®

AURIGA
the banking e-volution

www.aurigaspa.com

Si parla spesso degli attacchi informatici sui sistemi di home banking ma è giusto portare all'attenzione anche i rischi cyber a cui sono sottoposti i dispositivi ATM, che rappresentano l'anello più debole della catena dell'infrastruttura per la sicurezza bancaria, punto di accesso per i cybercriminali in tutto il mondo. Secondo l'analisi "ATMIA Global Fraud and Security Survey 2019" risultano infatti in aumento gli attacchi agli ATM: il 58% degli intervistati ha dichiarato una crescita sia delle violazioni della sicurezza fisica che delle frodi. Di quali attacchi stiamo parlando? Si tratta di Data Fraud (furto di dati personali, come ad esempio i numeri dei conti correnti e dei codici PIN), di Physical Fraud (attacco alle porte hardware allo scopo di estrapolare direttamente denaro contante) e di Cyber Fraud (attacchi logici ai sistemi e alle comunicazioni).

In particolare, ci sono cyber attacchi poco noti ma molti diffusi: ATM jackpotting, Skimmer e Transaction Reversal Fraud. Pensiamo per esempio all'ATM jackpotting, una delle tecniche meno complicate di ATM Malware Cyber Attack, nella quale si sfruttano le porte hardware dell'ATM affinché esso eroghi contanti tramite l'utilizzo del malware. La grande diffusione di questi attacchi è dovuta alla loro immediatezza nel raggiungere l'obiettivo e molte istituzioni finanziarie di tutto il mondo hanno perso ingenti somme a causa del jackpotting solo negli ultimi cinque anni. Tra i malware più diffusi e pericolosi vi è anche Ploutous, identificato per la prima volta in un ATM Cyber Attack in Messico nel 2013. Da allora ha generato perdite per più di 400 milioni di euro a livello mondiale. Mentre l'attacco con skimmer - il device capace di leggere, e in certi casi immagazzinare su una memoria EPROM o EEPROM, i dati della banda magnetica delle carte di credito - e il Transaction Reversal Fraud, solo in Europa, hanno generato dai 250 e i 350 milioni di euro di perdita ogni anno.

L'EAST (European Association for Secure Transactions) ha dichiarato che tali attacchi sono diventati la forma predominante di frode ATM in Europa, con oltre 5.000 incidenti nella prima metà del 2019, contro i poco meno di 2.000 dell'anno scorso, e che rappresentano il 45% di tutti gli attacchi commessi.

Perché questo avviene? Perché gli ATM risultano essere così vulnerabili? I motivi sono tanti e includono il fatto che gli ATM gestiscono informazioni sensibili (come numeri di carte di debito e credito, e codici di accesso ai conti), che si trovano spesso in ambienti non custoditi o insufficientemente monitorati e che sono dotati di scarse misure di sicurezza logica. Ma soprattutto dipende dalla diffusione di hardware e software obsoleti ed eterogenei nelle reti ATM. La scarsità di politiche di aggiornamento e l'uso diffuso di sistemi operativi non più aggiornabili rendono questi ambienti vulnerabili per natura. Teniamo conto che molti di essi si basano ancora su Windows 7, sistema operativo che non riceve più aggiornamenti dalla casa madre e di conseguenza non garantisce più la protezione verso nuove minacce. Si stima che su circa il 40% degli ATM in tutto il mondo sia installato ancora Windows XP (sistema operativo ancor più obsoleto di Windows 7) che non viene più supportato da Microsoft dal 2014, rendendo queste macchine ancora più attaccabili.

Infine, esiste un punto debole – molto più complicato – rappresentato dall'XFS layer, l'interfaccia standard progettata affinché il software applicativo multivendor possa essere eseguito sugli ATM indipendentemente dall'hardware in uso dalla banca. L'XFS layer utilizza API standard per comunicare con le applicazioni self-service; ciononostante, non è previsto un processo di autentificazione automatico, facendo in modo che i cyber criminali possano sfruttare l'interfaccia per avere accesso all'hardware dell'ATM - in particolare al cash dispenser per accedere al contenuto della cassaforte, al lettore delle carte per appropriarsi dei codici identificativi, e al tastierino per i codici PIN.

Da tutto questo si evince che le banche hanno necessità di implementare strategie di sicurezza mirate per gli ATM. Quando si tratta di sportelli bancomat, infatti, le tecnologie di protezione dell'endpoint generico - quali le soluzioni anti-malware - non sono sufficienti, poiché tali tecnologie nascono per proteggere i PC e i computer portatili. Gli ATM invece sono dispositivi critici perché non possono essere disconnessi per un determinato periodo di tempo per essere riavviati così come si fa con un dispositivo mobile.

Le reti e i sistemi degli ATM devono essere disponibili sempre - 24 ore su 24, 7 giorni su 7, per 365 giorni all'anno – e necessitano quindi di un approccio differente. Inoltre, i criminali informatici si sono dimostrati sempre molto innovativi nel creare nuovi attacchi locali mirati, che risultano meno rischiosi e molto più redditizi degli attacchi fisici tradizionali. L'applicazione di robuste ed efficaci contromisure di sicurezza per proteggere, monitorare e controllare gli ambienti ATM in maniera adeguata diventa quindi una necessità imprescindibile per il mondo bancario.

Per questo riteniamo che sia strategico per la banca adottare una soluzione di sicurezza centralizzata che protegga, monitori in tempo reale e controlli le reti e i dispositivi ATM. Attraverso un'unica piattaforma, le banche possono così prevenire i tentativi di utilizzo di malware o l'esecuzione di attività fraudolente su ATM infetti. Una soluzione di sicurezza ATM integrata, su diversi livelli di protezione, consente una gestione centralizzata della rete ATM e un'esecuzione remota di azioni, risparmiando tempo e risorse economiche. Per limitare quindi i rischi di cyber attacchi una buona piattaforma deve essere in grado di verificare in real time i requisiti hardware e software; proteggere le risorse, i dati, i processi e i dispositivi; effettuare un monitoraggio proattivo, generando alert su possibili frodi e attivando azioni specifiche di sicurezza a seconda dell'evento scatenante; verificare l'integrità di file e cartelle per impedire lo spoofing di file con scopi fraulenti; bloccare l'accesso non autorizzato alle risorse dei terminali self service; permettere la crittografia degli hard disk; facilitare le analisi forensi e azioni operative per anticipare o reagire a potenziali attività fraudolente; e, inoltre, monitorare le comunicazioni in entrata e in uscita per ogni processo degli ATM, indirizzo remoto, protocollo e porta, fornendo funzionalità di firewalling di alto livello.

Infine, l'ascesa del cloud computing e di servizi basati su cloud, che consentono di accrescere l'efficienza, la flessibilità e la velocità di risposta alle esigenze del mercato e allo stesso tempo la gestione di grandi quantità di dati, mette le banche di fronte a nuove sfide da affrontare. I servizi cloud consentono alle banche di migliorare la sicurezza dei loro dati e l'affidabilità dei loro sistemi, beneficiando di una potenza di calcolo significativamente maggiore, ma rendono necessario comprendere l'importanza di investire risorse per reagire di fronte a uno scenario di minacce in continua evoluzione, dove la cyber security deve diventare una priorità di business.

FONTE: CorCom (2020) – autore: Gianluigi Torchiani

OPINION PAPER

THE # NEXTGENBANK®

AURIGA
the banking e-volution

Auriga S.p.A.
Via Don Luigi Guanella, 17
70124 Bari - Italy
www.aurigaspa.com
headquarters@aurigaspa.com