Sicurezza nella Digitalizzazione dei Servizi Bancari: Sfide e Soluzioni



La digitalizzazione dei servizi bancari: sfide di sicurezza

La digitalizzazione dei servizi bancari e finanziari pone importanti sfide sul fronte della sicurezza: non a caso il tema è stato centrale nei lavori del Gruppo Cyber del G7, riunitosi in Italia lo scorso maggio proprio per individuare soluzioni condivise al rischio cyber che interessa le infrastrutture critiche nazionali e internazionali.

Numeri e tipologie delle minacce mirate al comparto finanziario

Il mondo *Finance*, già da diversi anni, si pone stabilmente al vertice delle classifiche relative ai settori più colpiti da attacchi informatici.

In base ai dati CLUSIT, *“nel 2023 il settore Financial/Insurance ha registrato il maggiore incremento di incidenti gravi nel nostro Paese, con il 9% di attacchi (era il 3,7% nel 2022)”*.

Le principali tipologie di minacce informatiche rilevate si confermano *Ransomware*, DDoS, *Phishing* e *Business Email Compromise* (BEC), veicolati da tecniche di *social engineering* rese sempre più sofisticate dall’Intelligenza Artificiale, insieme ad attacchi finalizzati alla sottrazione o al riciclaggio di criptovalute.

Secondo l'ultimo Global Crime Report dell'Interpol, una minaccia da non sottovalutare è poi rappresentata dalla diffusione del *"Financial Crime-as-a-service"* (FCaaS). Questa nuova forma di criminalità informatica offre servizi di attacco a pagamento, rendendo più facile per i cyber criminali organizzare attacchi complessi senza dover possedere competenze tecniche avanzate. Le organizzazioni criminali sviluppano e forniscono tecnologie e know-how per attività come il riciclaggio di denaro, le frodi e altre transazioni illegali. Con l'accelerazione digitale durante la pandemia, questo modello è diventato più sofisticato, consentendo ai cyber criminali di operare con maggiore efficienza e su scala globale.

Il panorama difensivo: un quadro preoccupante

Sul fronte della difesa, il panorama è allarmante. Un'indagine dell'International Monetary Fund rivela che oltre la metà delle Banche Centrali esaminate nel 2023 non ha ancora implementato una strategia nazionale per la sicurezza informatica del comparto finanziario. Questo lascia molte istituzioni vulnerabili agli attacchi, aumentando il rischio di interruzioni dei servizi e di perdite finanziarie significative.

LDM: La soluzione di Auriga per la sicurezza bancaria

In tale scenario, Auriga offre una vasta gamma di soluzioni a tutela delle infrastrutture e della continuità operativa aziendale: tra queste Lookwise Device Manager (LDM), piattaforma centralizzata per la protezione dei dispositivi ATM e ASST.

Consapevoli che gli sportelli bancari *self-service* sono bersagli appetibili per i criminali, LDM integra attività di

monitoraggio e rilevamento tempestivo di eventuali incidenti. Inoltre concentrando le operazioni di sicurezza su un'unica piattaforma, questa soluzione garantisce un impatto minimo sulle prestazioni dei dispositivi.

Basata sulla tecnologia brevettata Lookwise TECH e specificamente pensata per ambienti distribuiti, la piattaforma garantisce la massima modularità, scalabilità e flessibilità per adattarsi alle specifiche esigenze di ogni istituto, consentendo di sviluppare strategie di resilienza informatica solide e durature.

Il "caso 5B": una conferma della validità del modello LDM per il mondo Finance

Un esempio concreto dell'efficacia di LDM è rappresentato dalla società 5B, un importante player sudamericano che gestisce oltre 2.600 sportelli automatici in Guatemala, di cui il 25% appartenente a filiali bancarie.

Recentemente, 5B ha condotto un'analisi approfondita per definire una strategia di cybersecurity per garantire la sicurezza e la stabilità della rete ATM, dispositivi critici attivi 24 ore su 24 per 365 giorni all'anno.

Durante l'indagine, sono state identificate le seguenti esigenze prioritarie:

1. controllare tutte le operazioni ATM, inclusi i processi di manutenzione eseguiti da personale tecnico, spesso di terze parti;
2. minimizzare la potenziale superficie di attacco;
3. massimizzare il tempo di attività e disponibilità (*up-time*) degli sportelli automatici;
4. prevenire e monitorare eventuali minacce o attività impreviste *in loco*.

In particolare, i primi due punti presuppongono politiche di

sicurezza in base alle quali tutte le modifiche agli ATM (sia software sia hardware) devono essere autorizzate e monitorate. Questo per evitare configurazioni errate che potrebbero compromettere la qualità e la disponibilità del servizio, oltre a permettere di controllare e mitigare tempestivamente azioni illecite o dannose, come tentativi di eseguire software non autorizzato o di connettere dispositivi hardware non autorizzati.

I benefici di Lookwise Device Manager

Lookwise Device Manager garantisce il raggiungimento di questi obiettivi tramite:

- *whitelist* di software e hardware autorizzati, per evitare manipolazioni di file critici e impedire connessioni non autorizzate;
- crittografia del 100% dei dischi rigidi, mantenendo l'integrità di software e hardware;
- monitoraggio costante e rilevamento automatizzato di attività sospette;
- piani di risposta agli eventi imprevisti, inclusi controlli fisici e remoti.

Grazie a queste caratteristiche, LDM ha permesso a 5B di ottimizzare il tempo di attività dell'intera rete ATM, raggiungendo un'*up-time* del 98.4%.

La sicurezza come priorità nella digitalizzazione bancaria

La digitalizzazione dei servizi bancari e finanziari è inevitabile, ma comporta rischi significativi che devono essere gestiti con attenzione. Le soluzioni come Lookwise Device Manager di Auriga offrono una protezione robusta e flessibile, essenziale per affrontare le sfide di sicurezza attuali e future. Il caso di successo di 5B dimostra come un approccio proattivo alla cybersecurity possa garantire non

solo la protezione delle infrastrutture bancarie, ma anche la continuità del servizio.

Per saperne di più scarica il case study: Casi Studio e Storie di Successo dei Clienti – Auriga (aurigaspa.com)

Condividi sui Social Network: https://www.ictsecuritymagazine.com/notizie/sicurezza-nella-digitalizzazione-dei-servizi-bancari-sfide-e-soluzioni/