OT cybersecurity nella banking industry, trend 2022 tra sfide e soluzioni



Nell'ultimo biennio, il settore bancario ha affrontato profonde trasformazioni. Il proliferare di nuove operazioni digitali e la nascita di istituti di credito attivi esclusivamente online si sono rivelati fondamentali per offrire a persone e imprese un accesso costante ai servizi di pagamento e investimento, pur nell'impossibilità di recarsi fisicamente in filiale, soprattutto a seguito dell'impatto della pandemia su ogni modalità di vita e lavoro.

Avendo indubbiamente contribuito a migliorare la *usability* dei servizi, tutto lascia supporre che tale andamento proseguirà anche oltre il termine dell'emergenza sanitaria. Ma la migrazione digitale delle attività bancarie ha inevitabilmente aperto nuovi fronti di rischio; delineando uno scenario in cui conoscere le minacce e saper intercettare soluzioni tecniche innovative è fondamentale per poter erogare servizi efficienti, sicuri e all'altezza delle aspettative di mercato, in grado di proteggere tutti i punti di accesso che potrebbero diventare veicolo di minacce.

Cyber Security Threats e scenari di rischio nel settore bancario

Tra le aree maggiormente colpite dalle attività di *cybercrime* si annovera il *Finance/Insurance*, insieme a enti governativi e mondo ICT; proprio alle istituzioni bancarie e assicurative, infatti, era destinato oltre il 20% di tutti gli attacchi registrati nel 2021. Secondo alcuni studi il 70% delle violazioni aziendali ha origine negli endpoint.

E se i vari tipi di *malware*, soprattutto di tipo ***ransomware***, veicolati da vulnerabilità tecniche o errori umani, si confermano i principali vettori di attacchi sempre più severi e mirati, viene osservata un'accresciuta sofisticazione rispetto a truffe e furti d'identità condotti tramite attività fraudolente di tipo ***phishing***, ***smishing*** o **BEC** (*Business Email Compromise*).

Senza considerare le nuove tipologie di attacchi nate per insidiare le valute digitali.

Poiché i servizi finanziari risultano trasversali a tutti i settori, è evidente come l'aggiornamento di protocolli e policy di sicurezza vada considerato un'assoluta priorità se si desidera conservare la propria posizione sul mercato e tutelarsi, sul fronte economico e reputazionale, dalla preoccupante ascesa di un *Financial Cybercrime* sempre più organizzato.

Workstation, Remote workers, ATM e POS: come difendere l'infrastruttura bancaria

Nel settore bancario i rischi appaiono molteplici, così come gli *asset* coinvolti. Dalle postazioni dei dipendenti (in sede o da remoto, con un'ulteriore espansione della superficie da difendere) ai terminali ATM e POS, la distribuzione degli *endpoint* ha moltiplicato i punti d'accesso attraverso cui è virtualmente possibile raggiungere il cuore dell'organizzazione, imponendo nuove cautele anche e soprattutto in chiave di ***OT cybersecurity***.

A tal fine vanno sintetizzate diverse esigenze, tra cui:

- adottare un approccio *Zero Trust* alla sicurezza, soprattutto per i dispositivi critici (es. ATM), garantendone al contempo l'operatività e la necessaria manutenzione;
- prevedere il costante monitoraggio e la gestione in

tempo reale di tutti gli *access point*, con la possibilità di revocare o sospendere privilegi laddove risultino attività sospette (come manipolazioni dell'*hardware* o modifiche ai *software*);
- consentire l'immediato rilievo e conseguente analisi, a fini di *threat intelligence*, di eventuali anomalie nei comportamenti degli utenti o nel traffico di rete;
- implementare protocolli di intervento mirato per neutralizzare le conseguenze degli incidenti.

Cyber Incident Response: strategia difensiva e strumenti avanzati

Un panorama di rischio così articolato esige risposte altrettanto complesse: la formazione del personale e il monitoraggio costante delle reti, così come l'adozione degli strumenti tecnologici più avanzati – è il caso delle soluzioni *Cloud-based* – convergono tutte in una strategia di difesa che oggi dev'essere necessariamente dinamica e proattiva.

La piattaforma **Lookwise Device Manager** di Auriga, società europea leader nella fornitura di software e soluzioni tecnologiche per il mondo bancario e dei pagamenti, procede in questa direzione, integrando la protezione fisica e logica esercitata su ciascuna articolazione, centrale o periferica, dell'impresa. Questa soluzione offre diversi livelli di protezione in un'unica piattaforma, come la definizione di una procedura di whitelisting di processi eseguibili sull'ATM, che impediscono l'esecuzione di malware o software non autorizzati; la crittografia completa degli hard disk, che impedisce l'esecuzione di attacchi di reverse engineering, e la protezione dell'integrità del file system e dell'hardware.

Grazie a queste caratteristiche, la piattaforma LMD è un alleato ideale in un contesto in cui i leader della sicurezza sono chiamati a integrare le esigenze di prevenzione con la tempestività di risposta agli attacchi, con l'obiettivo di

limitare il più possibile i rischi informatici a garanzia della protezione dei dati e dell’infrastruttura bancaria.

Uno strumento flessibile, collaudato e certificato per la prevenzione e gestione di possibili attacchi; senza mai sacrificare – anzi agevolando – continuità e qualità dei servizi in modo da conservare la fiducia dei clienti, il più prezioso *asset* di ogni organizzazione.

A cura della Redazione

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/ot-cybersecurity-nella-banking-industry-trend-2022-tra-sfide-e-soluzioni/