

Zero Trust security per la banking industry



La sicurezza informatica è oggi un tema imprescindibile per le banche sia per la crescente digitalizzazione dei sistemi e dei processi, sia per la natura sempre più sofisticata dei cyber attacchi che, sempre più frequentemente, sfruttano il furto delle credenziali d'accesso ai sistemi bancari o di pagamento per arrivare a compiere transazioni fraudolente all'insaputa del cliente. Attività criminose la cui riuscita è spesso resa possibile dall'utilizzo di sistemi non aggiornati, dalle cattive pratiche di sicurezza informatica o dalla diffusione di campagne di disinformazione e fake news, circostanze che offrono il fianco a vettori di attacco tramite tecniche di ingegneria sociale.

Mai come in questo periodo storico, in cui la sicurezza informatica è fondamentale per la difesa del valore e degli asset delle imprese, oltre che per la protezione della nostra vita quotidiana, le banche hanno bisogno di infrastrutture protette, sicure e resilienti che blocchino i diversi tipi di attacchi provenienti dall'esterno in grado di paralizzare l'operatività dell'istituto o la raggiungibilità dei servizi digitali da parte dei loro clienti (per esempio con **attacchi di DDOS, Distributed Denial of Service**).

L'attacco **ransomware**, ad esempio, rappresenta negli ultimi anni per le banche una grande preoccupazione che amplifica le possibilità di danno legate all'infrastruttura ATM, poiché in grado di causare una grave interruzione del servizio con conseguenti perdite finanziarie e danni all'immagine dell'istituto stesso.

Tra le priorità delle realtà bancarie si afferma quindi la protezione del principale mezzo di erogazione del contante –

gli sportelli ATM – a tutela dei propri asset più sensibili, ovvero il denaro e le informazioni relative ai clienti.

I nuovi trend dell'ecosistema ATM

Per quanto le banche siano da tempo consapevoli di dover includere la sicurezza informatica nella propria agenda di business, l'evolversi delle tecnologie e parallelamente delle minacce impone di mantenere alta l'attenzione.

Attualmente, infatti, l'ecosistema ATM è interessato da diversi fenomeni:

1. crescente interconnessione ad altri sistemi, come la rete aziendale o gli archivi Cloud;
2. maggiore automazione e sofisticazione dei software utilizzati;
3. aumentata complessità delle operazioni malevole ad esso indirizzato

Va anche ricordato come gli ATM, elementi che compongono una rete *Self-service* in progressiva espansione, rappresentino la “prima linea” di difesa della filiale bancaria in quanto **dispositivi endpoint collocati prevalentemente all'esterno**. Phishing, furto di credenziali, malware indirizzati agli endpoint sono solo alcuni dei principali vettori di attacco che possono interessare un ATM, con conseguenze dirette in termini di perdite economiche e di fruizione del servizio, con ricadute anche sull'immagine della banca arrivando a rovinare la reputazione del marchio. È quindi evidente che la messa in sicurezza degli *endpoint* risulta fondamentale per garantire accessibilità, qualità e continuità dei diversi servizi erogati.

I vantaggi dell'approccio Zero Trust

In un contesto soggetto a così rapida evoluzione le soluzioni tradizionali, nate per proteggere ambienti più semplici del

settore bancario, non bastano.

I modelli basati sulla legittimità e sull'analisi comportamentale rischiano di lasciare aperte delle brecce: essi presuppongono infatti la conformità delle operazioni compiute da chiunque detenga i necessari privilegi di accesso. Ma da tempo i criminali informatici hanno imparato a introdursi nei sistemi tramite mezzi legittimi, spesso riuscendo ad aggirare i normali controlli di cybersecurity a difesa dei dispositivi *endpoint* (ATM, workstation, ASST).

Per di più, non prevedere un aggiornamento costante e proattivo delle policy di sicurezza significa lasciar circolare vulnerabilità già note, facilitando enormemente il lavoro degli attaccanti.

I due punti critici che con il modello Zero Trust si assolverebbero in ottica di un modello robusto di protezione ATM sono:

- Drastica riduzione della superficie di attacco: in modo che l'accesso sia consentito solo all'insieme minimo di risorse software e hardware legittime e strettamente necessarie al corretto funzionamento del dispositivo, sulla base di processi di certificazione delle risorse, attività e interazioni considerate affidabili in base alle esigenze operative di volta in volta individuate;
- Stretto controllo delle modifiche nell'ATM: pianificazione e costante aggiornamento di policy definite in base allo **stato dei dispositivi**, diverse a seconda che lo sportello sia in funzione e quindi accessibile ad attacchi, o che sia sottoposto a manutenzione; prevedendo in tal caso – a carico del personale tecnico di terze parti – specifici e rigorosi processi di autenticazione prima di consentire qualsiasi attività. Le modifiche al software, che vengono gestite centralmente, devono essere controllate in modo tale che solo i sistemi autorizzati possano apportarle,

mantenendo sempre il controllo dell'integrità del software distribuito.

LDM: la soluzione Auriga per i dispositivi critici

In applicazione del modello *Zero Trust* Auriga ha sviluppato Lookwise Device Manager, piattaforma centralizzata pensata per rispondere alle mutevoli esigenze di ambienti complessi come gli ATM, nonché per adattarsi a reti di ogni tipo o dimensione.

Oltre a sovrapporre diversi “strati” – come crittografia e *whitelisting* delle applicazioni – alla protezione integrale di hardware e dati, LDM applica una stringente policy di sicurezza anche alle operazioni di manutenzione affinché tutti gli interventi (a livello di software o di dispositivo) si svolgano in maniera controllata.

Dopo aver ridotto la superficie di rischio, il costante monitoraggio remoto ne fornisce una visibilità a tutto campo per consentire, in caso di rilevate anomalie, l'immediata attivazione dei più aggiornati protocolli di incident response. Nel settore bancario, l'obiettivo delle politiche di sicurezza non è solo minimizzare gli importanti costi economico-reputazionali legati agli attacchi informatici; ma è soprattutto offrire agli utenti la miglior *customer experience* possibile. *Lookwise Device Manager* lavora in questa direzione, facilitando l'operabilità dei sistemi e contribuendo ad allineare le strategie aziendali alle elevate aspettative dei clienti “digitali” di domani.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/zero-trust-security-per-la-banking-industry/>