Il self-service è sotto controllo

GRAZIE ALLA SOLUZIONE LOOKWISE DEVICE MANAGER, AURIGA PROPONE AL MERCATO BANCARIO UNA SOLUZIONE DI SICUREZZA OLISTICA, CHE INCLUDE ANCHE I DISPOSTIVI SELF-SERVICE. E PRESTO FARANNO CAPOLINO DELLE NOVITÀ, COME L'AI E L'ESTENSIONE DELLA SOLUZIONE AI POS

Una gestione centralizzata della sicurezza per la rete self-service. Ma non solo. Perché grazie a un concetto di cybersecurity olistica è possibile «proteggere, monitorare e controllare in tempo reale l'infrastruttura, le reti, i dispositivi self-service e le workstation degli operatori – afferma Rosvanna D'Amico, Product Engineer di Auriga –, anche da remoto».

Rosvanna D'Amico, Product Engineer di Auriga

Investire nella cybersecurity

Tutto questo grazie alla soluzione Lookwise Device Manager (LDM), integrata nella offerta di Auriga. «Gli attacchi crescenti all'infrastruttura self-service possono essere estremamente critici e minano la fiducia nei servizi bancari digitali – premette D'Amico. La corsa alla digitalizzazione delle banche e l'emergere di nuovi modelli di filiali hanno accresciuto gli asset da proteggere, attivando la necessità di adottare una strategia olistica per contrastare eventuali attacchi. Per questo motivo, abbiamo deciso di investire nella cybersecurity per offrire un pacchetto più completo di soluzioni».

Controllo da remoto...

Con chiari benefici per le banche: «risparmio di tempo e di risorse economiche, grazie a una gestione centralizzata della sicurezza della rete self-service – chiarisce D'Amico. Nel dettaglio, LDM è una soluzione OT (Operational Technology) di sicurezza centralizzata, modulare e multivendor, con un set completo di funzionalità volto a proteggere, monitorare e controllare l'intera infrastruttura bancaria. LDM, che si basa su principi NIST, offre diversi livelli di protezione in un'unica piattaforma, coprendo così tutti i tipi di attacchi informatici che possono verificarsi – spiega D'Amico. Inoltre, LDM consente di mettere in atto efficaci azioni di monitoraggio degli eventi e di controllo dell'apparecchiatura da remoto».

... grazie al whitelisting

Il controllo da remoto è regolato da un «concetto di whitelisting, per consentire l'accesso alle risorse del sistema in maniera controllata – continua D'Amico. Ma non meno importante è la prevenzione, rilevamento e risposta a incidenti di sicurezza, compresa la protezione da attacchi fisici-logici: la gestione centralizzata permette quindi di gestire tutti gli alert di sicurezza e visualizzare, su un'unica piattaforma, i report in tempo reale sullo stato degli ATM e delle workstation degli operatori».

In arrivo AI e protezione per i POS

E all'orizzonte si prospettano due novità per la sicurezza targata Auriga. Da una parte l'AI, dall'altra l'estensione della soluzione LDM anche ai POS. «L'intelligenza artificiale può infatti essere utilizzata per la raccolta e l'analisi di informazioni al fine di caratterizzare possibili minacce cyber e per prevenire potenziali criticità. I POS, invece, per loro natura sono altamente vulnerabili ad attacchi criminali o azioni fraudolente mirate – conclude D'Amico. Un sistema di whitelisting basato sul controllo delle applicazioni e dei dispositivi hardware autorizzati, consentirà di aumentare il livello di confidenza nell'uso di questa apparecchiatura».

G.C.