# Le sfide del cyber crime

Rosvanna D'Amico è product engineer di Auriga, società che progetta e realizza software per le banche. Durante l'evento online dedicato alla sicurezza delle apparecchiature ATM, D'Amico ha focalizzato il suo intervento innanzitutto sul tema della cybersecurity. «Gestiamo 40 mila dispositivi self service e 100 miliardi di transizioni annue. Secondo l'European Association for Secure Transaction (Esta), il costo dei crimini informatici per l'economia globale è di 400 miliardi di dollari all'anno. Gli attacchi cyber di tipo malware in Europa sono stati 5 mila solo nella prima metà del 2019, contro poco di 2 mila del 2018. Il 45% è stato rivolto agli ATM, con perdite riportate in crescita del +142%».
Le criticità degli ATM sono diverse: «L'impatto notevole alla sicurezza è dato da sistemi operativi obsoleti: in contrapposizione all'ascesa del Cloud, il 40% utilizza Windows XP, non più manuntenuto da Microsoft dal 2014 e ormai privo di aggiornamenti di sicurezza. In secondo luogo, lo strato XFS rappresenta una vulnerabilità estrema per l'accesso non strutturato. Terzo, pesa l'esposizione dei componenti hardware, poiché gli ATM si trovano in ambienti poco custoditi e monitorati. Infine, gli ATM contengono dispositivi Fix - Purpose che devono garantire il corretto funzionamento del terminale: un anti-malware potrebbe essere insufficiente, perché, a fronte di una frode, bisogna garantire un'alta operatività costante».
Le caratteristiche di una soluzione di cyber security applicata agli ATM sono ben definite. «Le banche devono agire in modo ciciclo, gestendo i rischi fisici e logici in un processo di miglioramento continuo». Il riferimento sono le linee guida del Nist, il National Institute of Standards and Technology, il primo a diffondere il termine di cyber security. «La strategia di difesa prevede quattro momenti: "analizzare" il contesto in cui si opera, definendo il piano operativo per gestire al meglio gli attacchi; "proteggere" sviluppando e attuando controlli una volta identificate le lacune del sistema; "rilevare", nel senso di implementare le attività per identificare il verificarsi di un evento di sicurezza informatica; infine "rispondere", verificando che le azioni di sicurezza di fronte a un evento cyber siano efficaci, ripristinando eventualmente le periferiche. Tale processo deve essere continuo».
D'Amico ha concluso il suo intervento con un consiglio. «Suggeriamo alle banche di adottare una soluzione centralizzata, pronta a proteggere e monitorare in tempo reale tutti i dispositivi self-service, garantendo una operatività di 24 ore per 365 giorni all'anno».

**Rosvanna D'Amico,**
product engineer, Auriga