Sommario

1. Scenario in evoluzione di minacce e rischi

In un processo di risk assessment e management i rischi vengono parametrati sul valore degli asset da proteggere e sulle probabilità di occorrenza di eventi a rischio.

Nello scenario corrente aumenta il valore dell'asset "clienti" e "operatori", in termini di safety e security.

Le dipendenze si stanno rapidamente trasformando, in "filiali salotto", dove si effettua principalmente consulenza e vendita di prodotti finanziari e assicurativi, con le operazioni di cassa sempre più delegate prevalentemente a sportelli automatici o Atm evoluti, mentre gli operatori di front-office tendenzialmente non tratteranno fisicamente il contante.

1.1. Sicurezza logica e fisica

La linea di demarcazione fra sicurezza logica e fisica, nelle tradizionali accezioni, si fa sempre più labile, in presenza di aree self-service che possono gestire sia il prelievo che il versamento di contanti, ma anche l'accesso informativo/dispositivo in rete ai sistemi della Banca tramite chioschi e/o ATM evoluti.

1.2. Nuovi modelli di filiale

I nuovi modelli di filiale unattended h24 generano nuove e diverse esigenze per preservare safety e security dei clienti.

1.1. I sistemi di protezione perimetrale

I sistemi perimetrali sono in evoluzione e spesso vengono eliminate le barriere fisiche all'entrata delle aree "open" accessibili liberamente da clienti o potenziali clienti.

1.2. Le minacce prevalenti e incombenti

Le minacce per rapine e furti sono diminuite (-82% dal 2007 a fine 2015), mentre stanno crescendo le minacce per atti vandalici e/o di matrice terroristica potenzialmente indirizzate non solo alle location aperte al pubblico, ma anche a sistemi di elaborazione centrali e a siti di business continuity, comprese le reti di comunicazione fra sistemi e con le utenze interne ed esterne, queste ultime di norma su reti "pubbliche" e attestate su centrali di telecomunicazione di dubbia sicurezza.

1.3. Locations custodia valori

Diventa allo stesso tempo sempre più critica la protezione di location dedicate alla custodia valori (cassette di sicurezza, grandi caveau propri e presso terzi), che sono ormai il target preferenziale di attacchi fisici, spesso integrati con attacchi logici/intrusione/insiding alle strutture di sorveglianza e controllo, con conseguenze economiche e reputazionali potenzialmente devastanti.

1.4. Rischi su ATM

Gli ATM "fronte strada" sono soggetti a frequenti aggressioni/furti, ed anche la clientela è esposta ad attacchi o truffe presso gli ATM.

2. Scenario in evoluzione degli strumenti tecnologici e logici innovativi

2.1. Banda e virtualizzazione

La tecnologia allo stato dell'arte, unita ad una grande disponibilità di banda a basso costo, consente di "virtualizzare" alcune funzioni attualmente delegate alle centraline locali di sorveglianza e controllo, garantendo livelli di servizio estremamente elevati, uniti ad abbattimento dei costi di manutenzione e gestione locale.

2.2. Tecnologie di "homeland security"

Per proteggere efficacemente aree poco presidiate si stanno diffondendo tecnologie sofisticate, attualmente usate soprattutto in contesti di "homeland security"e infrastrutture critiche, in ambito civile e militare, che consentono, oltre alla consueta registrazione audio/video:

- il riconoscimento facciale di individui, mettendolo a confronto con database di "segnalati", anche di identità sconosciuta, che abbiano mostrato comportamenti anomali;
- il riconoscimento ed il comportamento di veicoli che ripetutamente si avvicinano al luogo da proteggere;
- il riconoscimento "di scena", individuando situazioni di potenziale pericolo anche in ambienti "unattended", ed allertando le centrali di controllo e supervisione in tempo reale;
- Il riconoscimento di "oggetto abbandonato", di "uomo a terra", etc., che sono prerogativa funzionale dei sistemi più evoluti di analisi intelligente audio/video, già adottati con successo in ambienti ad alto rischio, come porti/aeroporti, stazioni ferroviarie, infrastrutture critiche e grandi eventi.

2.3. Uso di sistemi di AI ad elevata potenza

Sistemi ad altissima potenza di calcolo, utilizzabili in architettura "cloud" as service, possono validamente correlare in tempo reale, in maniera semantica, un evento (o una sequenza di eventi) con milioni di altri eventi simili, per "pesarne" il potenziale di rischio ed effettuare segnalazioni alla centrale di sorveglianza, minimizzando il numero dei "falsi positivi", che generano costi molto elevati per la loro gestione.

3. Attività preliminari da esperire

Per poter formulare un progetto efficace, prestazionale ed economico, con l'obiettivo di migliorare i livelli di servizio, adeguandoli ai nuovi scenari di rischio, occorre mettere in atto una serie di interventi conoscitivi preliminari, come parte integrante e preliminare del progetto:

3.1. Overview sul campo

Overview sul campo delle attuali locations e impianti, strutture di protezione interne e perimetrali, con la logica di adeguarli alle nuove necessità di protezione (personale, clienti e valori) contro minacce anche di carattere vandalico e/o terroristico.

3.2. Progetto di revisione infrastruttura

Progetto di revisione layout fisico, controllo accessi, collocazione dispositivi di controllo e di rete, inclusi i punti di derivazione delle Telcos.

3.3. Analisi dei processi

Presa d'atto dei processi esistenti, vulnerabilità e risk assessment e revisione/adattamento dei processi attuali.

3.4. Revisione processi

Progetto di interventi sulla struttura organizzativa, in particolare per le sedi a minor presidio umano e per il presidio del centro di controllo. Validazione e revisione processi per accesso da terze parti (impiantisti/manutentori, sorveglianza esterna, etc.) delle strutture sensibili.

3.5. Distribuzione elettrica e backup

Valutazione sistemi attuale di backup elettrico e di distribuzione agli apparati di campo e loro eventuale revisione.

3.6. Valutazione parco telecamere e sensori

Valutazione del parco installato videocamere analogico e IP, proposte di standardizzazione e/o di riuso/sostituzione, valutazione ed inventario dei sensori ambientali, valutazione di nuove esigenze eventuali di copertura e rilevamento allarmi, anche generati da analisi video intelligente.

3.7. Valutazione mappatura e disponibilità reti mobili LTE/4G+

Valutazione della disponibilità, del costo/beneficio e dell'opportunità d'uso di reti LTE/4G+ come backup o primarie (analisi, per ciascuna location, di forza e qualità del segnale e banda di upload disponibile e/o garantita).