

EVOLUZIONE TECNOLOGICA IN FILIALE

Le filiali bancarie sono dotate di tecnologie sempre più sofisticate, che aumentano l'efficienza e la sicurezza e favoriscono il contatto con i clienti, trasformandosi così da luogo dedicato alle transazioni economiche a vere e proprie piattaforme relazionali

Negli ultimi anni le filiali bancarie hanno cambiato volto e si sono trasformate da “templi del denaro” in punti di contatto multifunzionali, sono state introdotte le “agenzie leggere”, che hanno permesso di portare i servizi bancari più vicini ai cittadini, mentre un utilizzo sempre più spinto delle tecnologie dell'informazione e delle telecomunicazioni ha permesso di aumentare notevolmente l'efficienza e la sicurezza delle transazioni.

In un primo tempo le tecnologie sono state utilizzate per blindare le filiali con le bussole automatiche all'ingresso, spesso dotate di metal detector e/o di lettore di impronte digitali, per sostituire i *vigilantes* che prima presidiavano l'ingresso. Recentemente, con l'adozione delle casseforti temporizzate, dei roller cash e dei cash-in/cash-out a disposizione dei cassieri, la diminuzione del contante circolante e la maggiore importanza delle funzioni di consulenza, si tende a semplificare l'accessibilità realizzando “filiali aperte”, senza bussole all'ingresso e con un contatto più diretto tra clienti e impiegati della banca, favorito anche dalla maggiore quantità di informazioni e di servizi disponibili online: un nuovo *concept* che abbate le barriere all'ingresso e rende tutto più semplice, veloce e sicuro, perché la sicurezza viene spostata dove si trova fisicamente il denaro, e diminuisce la

distanza col cliente secondo nuovi modelli di interazione. Le banche tendono quindi ad avere filiali efficienti, con aree self-service, sicurezza allo sportello e spazi per la comunicazione dinamica, anche tramite tecnologie innovative come il *Digital Signage* (cartellonistica elettronica) e la comunicazione multimediale.

Queste sono espressioni di una tendenza allo snellimento delle procedure di accesso in senso generale (ai dati, ai sistemi, alle filiali), che però non deve andare a detrimento della sicurezza in tutte le sue dimensioni (sicurezza dei clienti, dei dipendenti, dei valori e dei dati, intesa sia come *safety* che come *security*). Il sistema di sicurezza non deve essere percepito come invasivo o lesivo della privacy e deve causare il minor disagio possibile. Il problema sul tappeto è quindi garantire un livello congruo di accessibilità senza compromettere la sicurezza globale. La filiale bancaria evolve da luogo dedicato alle transazioni a piattaforma relazionale: deve quindi essere un luogo confortevole e accogliente dove il cliente può ottenere assistenza, informazioni sui prodotti e consulenza.

Poiché una banca non può funzionare se il sistema informativo non è accessibile, anche il funzionamento delle stazioni di lavoro, della rete e delle linee di comunicazione è di importanza critica quanto la sicu-

rezza. Con la diffusione delle reti geografiche a banda larga (cablate e wireless), delle reti IP e di dispositivi in grado di collegarsi alle reti locali Ethernet, la dotazione tecnologica delle agenzie ha cambiato volto ed è diventata molto più complessa e critica per il funzionamento della banca: una moderna filiale è un concentrato di impianti e apparati tecnologici, notevolmente più complessi e critici rispetto a quelli di un normale ufficio. Nel seguito, passiamo in rassegna i principali sottosistemi che consentono di garantire la sicurezza attiva logica e fisica delle agenzie bancarie.

SISTEMA INFORMATIVO

L'attuale tendenza è quella di eliminare i server dalle filiali, per aumentare la sicurezza e semplificare la gestione. Quindi nelle filiali ci sono generalmente solo stazioni di lavoro collegate tramite linee dati ai server installati nei data center remoti. Nei posti di lavoro delle casse sono utilizzati PC o WBT (Windows Based Terminal), dotati di stampante ad aghi e di lettore di assegni (*scanner*), che spesso, oltre a leggere i codici magnetici MICR, acquisiscono anche le immagini degli assegni stessi, che sono gestite da molti sistemi applicativi bancari per l'archiviazione ottica e per il controllo della firma.

Sono in forte crescita gli sportelli dotati di cash dispenser (cash-in/cash-out) collegati alla LAN. Questi apparecchi sono costituiti da una cassaforte temporizzata in cui vengono immesse tutte le banconote depositate dai clienti e da cui vengono prese le banconote da consegnare ai clienti che prelevano. Poiché "vedono" passare tutte le banconote, questi dispositivi possono effet-

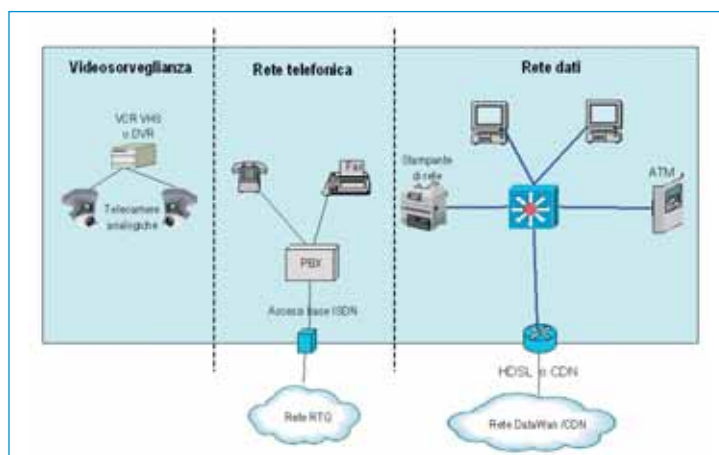


Figura 1 - Filiale di tipo tradizionale – Impianti separati

tuare varie funzioni oltre alla pura custodia delle banconote. Se sono integrati con l'applicativo bancario, possono effettuare la gestione fisica completa dei contanti. Inoltre, grazie ai sensori di cui sono dotati, riconoscono le banconote false e quelle usurate che devono essere rese alla Banca d'Italia, e producono tutti i rapporti relativi ai flussi di contante, banconote false e banconote riciclate.

Tutti i nuovi bancomat (ATM) sono in grado di gestire le carte bancomat con microchip, eseguono decine di transazioni, si collegano in rete con il protocollo IP e sono predisposti per ospitare al loro interno una telecamera protetta. In tutte le filiali c'è almeno una stampante laser di rete multifunzione.

RETE VOCE E DATI

Le filiali "leggere", che ospitano tipicamente da una a dieci persone, sono collegate a reti a banda larga di tipo tradizionale (come Datawan di Telecom Italia) o MPLS tramite linee principali HDSL e linee di backup ADSL o ISDN. Sono quasi scomparse le costose e lente vecchie linee dedicate punto-punto (CDN e CDA), che sopravvivono solo nei piccoli

centri non ancora serviti dalla banda larga.

Talvolta sono utilizzati anche collegamenti in fibra ottica o ponti radio (prevalentemente Hiperlan per distanze di alcuni chilometri e ponti laser per collegamenti tra edifici poco distanti).

La filiale è collegata alla rete tramite un router (a cui si può affiancare un router di backup), spesso dotato di firewall e di funzioni di crittografia dei dati (VPN) per creare un collegamento sicuro con la sede.

Ogni filiale bancaria moderna è dotata di una LAN Ethernet, a cui si collegano vari apparati e impianti. I server di filiale spesso vengono eliminati, poiché c'è un deciso orientamento ad accentrare i server presso i data center (di proprietà delle banche o in outsourcing) per risolvere i problemi di sicurezza e di gestione. Le stazioni di lavoro di sportello e di back office sono basate su PC o Windows Based Terminal, spesso affiancati da dispositivi cash-in/cash-out utilizzati dai cassieri. Alla LAN di filiale si collegano inoltre stampanti laser e multifunzione, Bancomat IP, centralini telefonici VoIP, Videoconferenza/videocomunicazione, totem con varie funzioni (quotazioni di borsa, interrogazione dei documenti sulla trasparenza bancaria), terminali per rilevazione presenze e controllo accessi, gateway dei sistemi di sicurezza locale (antintrusione, antincendio, controllo climatizzazione). Il cuore della LAN è costituito da uno switch Ethernet, tipicamente a 10/100 Mbps. La disponibilità di schede di rete a 1 Gbps su tutti i nuovi PC consiglia di adottare switch a 1 Gbps anche nelle piccole filiali. È anche consigliabile utilizzare switch gestibili (*managed switch*) per poter controllare dal centro le LAN delle filiali e

individuare i problemi tramite assistenza remota.

L'alimentazione elettrica ad alcuni apparecchi come telefoni IP, access point e telecamere IP può essere fornita anche dalla rete Ethernet, utilizzando appositi switch POE (Power Over Ethernet), in grado di iniettare la tensione di alimentazione sul cablaggio strutturato. Le filiali moderne sono dotate di cablaggio strutturato per la distribuzione di voce, dati e immagini.

Le filiali di tipo tradizionale sono dotate di un centralino telefonico ISDN. Il fax può essere collegato a un interno del centralino o direttamente a una linea telefonica indipendente. Molte banche hanno in corso progetti pilota per valutare la telefonia IP (VoIP) e alcune hanno già introdotto la telefonia IP in tutte le filiali, collegando i telefoni IP direttamente agli switch della LAN o utilizzando centralini telefonici ibridi, in grado di collegare sia telefoni tradizionali che telefoni IP.

SISTEMI DI SICUREZZA

Attualmente, le filiali sono dotate prevalentemente di sistemi di videosorveglianza basati su telecamere analogiche e di sistemi di videoregistrazione digitale su disco (DVR o *Digital Video Recorder*), spesso collegati in rete e interrogabili dal centro o da una società di sorveglianza esterna. Iniziano a diffondersi le telecamere a colori, le telecamere panoramiche "a cupola" (*dome camera*) e le teleca-

mere IP, fisse o brandeggiabili (DMZ), spesso dotate di funzioni di riconoscimento dei movimenti (*motion detection*) e integrate con i sistemi di allarme. Si iniziano a utilizzare anche telecamere intelligenti in grado di riconoscere se chi entra ha il viso mascherato, di contare i clienti presenti e di ricostruirne i movimenti. Spesso i sistemi di videosorveglianza sono chiusi in cassaforte e sono dotati di gruppi di continuità dedicati, chiusi anch'essi in cassaforte. In altri casi,

i DVR sono installati insieme agli apparati di rete e alimentati dal medesimo UPS.

Le filiali sono generalmente dotate di sistemi antincendio con rivelatori di fumo collegati all'impianto di allarme. Gli impianti antintrusione sono collegati a istituti di vigilanza o alle forze dell'ordine tramite linee telefoniche e collegamenti GSM. Spesso impianti antintrusione, impianti antincendio e di videosorveglianza sono integrati.

Il trend delle installazioni di dispositivi biometrici per controllare gli accessi alle banche (soprattutto riconoscimento delle impronte digitali), evidenzia una tendenza al decremento, dovuta principalmente alla normativa restrittiva imposta dal Garante della Privacy, alla scarsa affidabilità e al fatto che ritardano l'ingresso dei clienti in filiale. I controlli biometrici sono invece applicati maggiormente nei siti a rischio elevato, come le sale macchine dei CED, nel qual caso si utilizzano anche tecnologie più sicure delle impronte digitali, come il riconoscimento dell'iride, del volto o della geometria della mano.

IMPIANTO ELETTRICO E DISPOSIZIONE FISICA

Per garantire il corretto funzionamento delle apparecchiature informatiche e della rete voce e dati, le filiali devono essere dotate di gruppi di continuità elettrica (UPS - *Uninterruptible Power Supply*), e di impianti elettrici privilegiati, normalmente contraddistinti da prese rosse, per distinguerle dalle prese

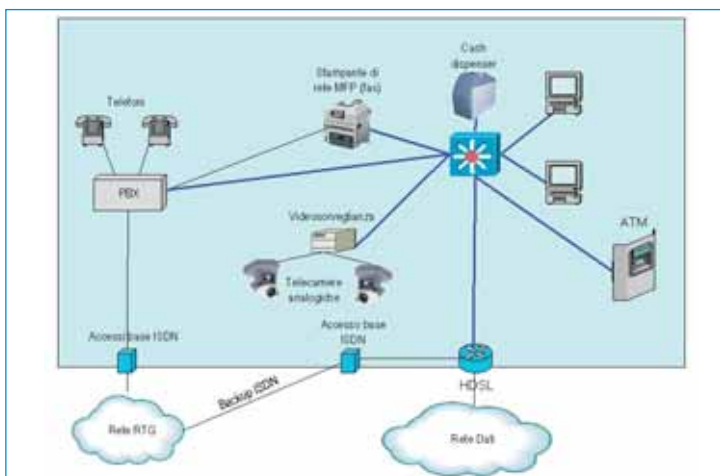


Figura 2 - Filiale parzialmente integrata - Telefonia IP e videosorveglianza in rete

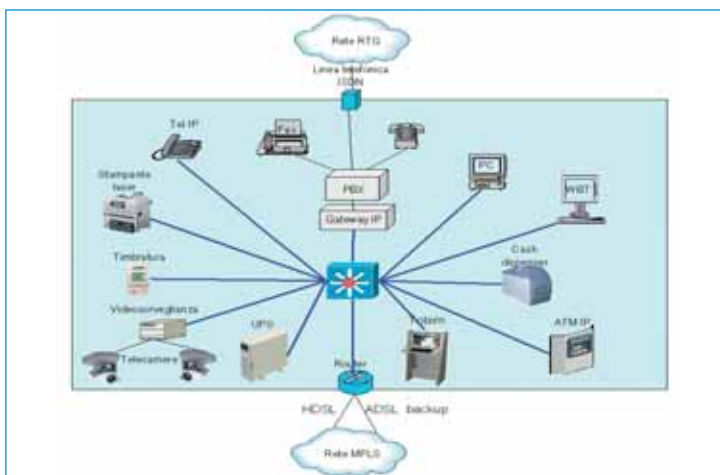


Figura 3 - Filiale completamente integrata

dell'impianto elettrico principale. All'impianto privilegiato, alimentato dall'UPS, tipicamente si collegano: gli apparati di rete, gli apparati dei posti di lavoro (PC o WBT, lettore di assegni, stampante, cash-in/cash-out), i terminali self-service e i totem informativi, il bancomat, l'impianto di videoregistrazione e il centralino telefonico (se non è già dotato delle proprie batterie). Normalmente non si collegano stampanti laser e fotocopiatrici, a causa dagli alti assorbimenti elettrici.

È buona norma radunare in un vano tecnico tutti gli impianti tecnologici di tipo elettrico ed elettronico (quadri elettrici, pannelli di permutazione del cablaggio strutturato, router, switch, UPS, videosorveglianza, impianti di allarme, controllo accessi,

etc). Spesso nello stesso vano sono installati anche i sistemi di climatizzazione e altri sistemi di controllo ambientale, che sempre più spesso vengono integrati in rete.

TRE STADI EVOLUTIVI

Non tutte le filiali sono organizzate secondo un modello completamente integrato, che di solito viene realizzato nelle filiali di nuova apertura o in seguito a ristrutturazioni. Attualmente coesistono tre stadi evolutivi:

1. **Filiali tradizionali**, in cui impianti telefonici, rete dati e impianti di sicurezza sono indipendenti (Figura 1)
2. **Filiali in uno stadio intermedio**, in cui ci sono vari livelli di integrazione: tipicamente telefonia IP e/o videoregistratori digita-

li per la videosorveglianza e/o gruppi di continuità elettrica controllati in rete (Figura 2)

3. **Filiali completamente integrate**, in cui la rete IP concentra tutte le funzioni di comunicazione, gestione delle transazioni e controllo logico e fisico (Figura 3).

La tendenza generale è comunque verso l'integrazione in rete di tutti i principali dispositivi e sottosistemi, poiché le soluzioni integrate offrono notevoli vantaggi in termini di risparmi sui costi di rete, possibilità di controllo e monitoraggio remoto, telediagnosi e telemanutenzione, maggiore efficienza e sicurezza, che concorrono a migliorare l'immagine dell'istituto di credito e i rapporti con i clienti.