

A banner image showing a modern glass skyscraper with the text "Intesa SanPaolo – Security Assessment" overlaid in white. The background is a blue-tinted photograph of the building's facade.

# Intesa SanPaolo – Security Assessment

## **Il cliente**

Intesa Sanpaolo è il gruppo bancario nato dalla fusione di Banca Intesa e Sanpaolo IMI, due grandi realtà bancarie italiane caratterizzate da valori comuni che si sono aggregate per crescere, per servire meglio le famiglie e per contribuire ulteriormente allo sviluppo delle imprese e alla crescita del paese. Intesa Sanpaolo è leader in Italia in tutti i settori di attività (retail, corporate e wealth management). Il Gruppo offre i propri servizi a 11,9 milioni di clienti avvalendosi di una rete di circa 4.400 sportelli presenti su tutto il territorio nazionale con quote di mercato non inferiori al 12% nella maggior parte delle regioni. Intesa Sanpaolo ha una presenza internazionale strategica, con circa 1.100 sportelli e 7,5 milioni di clienti, incluse le banche controllate operanti nel commercial banking in 12 Paesi dell'Europa centro-orientale e nel Medio Oriente e Nord Africa, e una rete internazionale specializzata nel supporto alla clientela corporate in 25 Paesi, in particolare nel Medio Oriente e Nord Africa e in quelle aree in cui si registra il maggior dinamismo delle imprese italiane, come Stati Uniti, Brasile, Russia, India e Cina.

## **Sito web**

[www.group.intesasanpaolo.com](http://www.group.intesasanpaolo.com)

## **Settore Merceologico**

BANCARIO



A banner image showing a modern glass skyscraper with the text 'Intesa SanPaolo – Security Assessment' overlaid in white.

# Intesa SanPaolo – Security Assessment

## Dati case history

Intesa Sanapolo si è rivolta a Betacom per servizi di security assessment, che includono vulnerability assessment e penetration test dell'infrastruttura e delle applicazioni.

Betacom ha provveduto al Vulnerability Assessment per la valutazione della sicurezza informatica, che consiste nell'individuare il maggior numero di vulnerabilità presenti in uno o più sistemi informatici, fornendo un'indicazione di massima del loro impatto e delle possibili contromisure.

Successivamente sono stati svolti Penetration Test simulando un reale tentativo di attacco sfruttando le vulnerabilità emerse in fase di Vulnerability Assessment.

Il Penetration Test applicativo è stato effettuato in modalità manuale sia in modalità black box che in modalità grey box.

## Dettagli soluzione

- Valutazione dei rischi dei sistemi
- Individuazione delle criticità sistemistiche.
- Chiusura dei banchi
- Maggiore sicurezza dei sistemi.

## Benefici ottenuti

- Analisi dei sistemi in connessione remota con tecniche di ethical hacking

