

SOLUZIONE PER ANTIFRODE

Proteggere efficacemente il proprio online banking è una sfida importante. Le minacce dal fronte cyber crime diventano sempre più **numerose e sofisticate**. Per contrastarle occorre dotarsi di strumenti all'avanguardia, che si possano affiancare alle soluzioni di sicurezza già utilizzate e che concorrano ad elevare il livello globale di protezione.

Questa soluzione è basata sull'analisi comportamentale che permette di rilevare e gestire le operazioni fraudolente in ambito bancario.

l'esigenza

Avere uno strumento di sicurezza, in grado di **prevenire frodi ai propri sistemi di online banking**, contrastando in modo efficace sia le attuali che le future minacce da parte del cyber crime.

Coprire tutte le necessità di chi deve operare all'interno di un gruppo di **fraud detection**: monitoraggio delle transazioni, riconoscimento delle frodi, investigazione, migliorando nel contempo l'efficienza dell'intero team.

Avere uno strumento di **facile integrabilità con la propria infrastruttura applicativa**: dal punto di vista tecnico, per non aggiungere complessità al sistema stesso e dal punto di vista dell'operatività, in modo da non stravolgere il consueto modo di operare sul front end applicativo da parte degli utenti finali.

Avere la possibilità di utilizzo anche in modalità real-time per una **azione tempestiva di prevenzione e di rafforzamento** della sicurezza con l'obiettivo finale di **ridurre le perdite economiche e mantenere la fiducia della propria clientela**.

la soluzione

Il "core" della soluzione è costituito da un sistema esperto (Risk Score Engine). Questo componente è in grado di **"imparare a riconoscere" i clienti finali**, basandosi su oltre un centinaio di parametri che li caratterizzano in modo univoco.

Dall' "impronta digitale" dei dispositivi usati, ai parametri del "canale" su cui vengono fatte le richieste, fino alla geolocalizzazione dell'utente: tutte queste informazioni vengono correlate e confrontate con i comportamenti statistici degli utenti stessi, calcolando un fattore di rischio per ogni transazione richiesta. Questo valore può quindi essere utilizzato, nei casi di transazioni sospette, per far scattare le varie contromisure previste. Dall'intervento del personale interno per ulteriori investigazioni, alla richiesta di ulteriori meccanismi di autenticazioni, ad esempio basati su SMS o challenge del tipo domanda/risposta definiti dagli utenti.

La soluzione prevede inoltre un'applicazione di Case Management per la **gestione completa degli incident di sicurezza**, la componente Policy Manager che permette anche la **creazione di policy personalizzate** e la reportistica.

La suite può utilizzare inoltre i servizi di supporto e FraudNetwork che permettono di usufruire in real time dei parametri (ad es. black list di IP address) utili ad aumentare l'efficacia della rilevazione delle transazioni fraudolente.

i vantaggi

La soluzione è in grado di **ridurre in modo significativo i costi legati alle transazioni fraudolente**. Le statistiche indicano infatti una percentuale variabile tra il 60 e 80% di riconoscimento di transazioni illecite.

Rafforza la parte di autenticazione, grazie alla possibilità di utilizzare ulteriori sistemi Out of Band (One Time Password inviata tramite GSM), per i casi in cui esistano dubbi sulla parte di autenticazione.

Prevede un sistema di **integrazione semplificata** con l'infrastruttura esistente, grazie alla varie possibilità che il prodotto mette a disposizione: Web Services, hidden Html, elaborazione di log files applicativi.

Essendo basata su algoritmi di analisi comportamentale la soluzione è in grado di **fronteggiare anche le nuove tipologie di attacco** che si presenteranno nel prossimo futuro. Non si tratta infatti dell'applicazione di regole statiche che devono essere aggiornate periodicamente, ma di un sistema in grado di apprendere dai feedback che riceve dal gruppo di gestione anti frode.

Offre una serie di strumenti che permettono di gestire in modo rapido l'individuazione e la risoluzione dei vari incident, permettendo di **ottimizzare l'attività di verifica**.

E' un **layer "trasparente"**, che non comporta nessun cambiamento alla consueta modalità di utilizzo, se non nel caso di transazioni sospette che richiedano ad esempio una seconda prova di autenticazione.

About IKS

IKS, nata alla fine degli anni novanta focalizzando il proprio agire sui principali temi dell'Information e Communication Technology, è in grado di fornire servizi e soluzioni utili a migliorare i processi aziendali, con competenza e approccio innovativi. IKS può vantare tra i propri Clienti le principali aziende del panorama nazionale.

Alcune idee maturate nel corso di esperienze reali sono diventate "soluzioni a valore" che permettono di proporsi sul mercato in modo esclusivo.

www.iks.it
informazioni@iks.it
+39 049.8701010

padova
corso Stati Uniti, 14 bis - 35127



appassionati all'eccellenza