



## Collaborazione e comunicazione

**In occasione del Security Summit di Milano, gli esponenti del mondo bancario hanno potuto confrontarsi in una tavola rotonda sul tema della sicurezza del cliente moderata da Anthony Cecil Wright, presidente di Anssaif**

Nell'accedere ai canali informativi e dispositivi, via Atm e web, offerti dagli intermediari finanziari, il cliente è sempre più consapevole del rischio dovuto all'esposizione a potenziali frodi tramite tecniche sofisticate. Tuttavia, tali rischi possono essere enfatizzati presso l'opinione pubblica a causa non tanto della mancanza di tecnologia necessaria a contrastarle, quanto piuttosto per una scarsa capacità o volontà del sistema bancario a comunicare all'utente finale i vantaggi e le caratteristiche dei nuovi dispositivi. Da qui, la diffidenza e la scarsa propensione a utilizzare il canale

on line per effettuare alcune operazioni. Ma come superare tale "impasse", fermo restando l'impegno comune nel migliorare le misure di sicurezza a tutti i livelli? A tale quesito hanno provato a rispondere i partecipanti alla tavola rotonda "L'attenzione delle banche alla sicurezza del cliente: da un approccio cost oriented alla crescita di valore", che si è tenuta a Milano in occasione del Security Summit (v. box). **Anthony Cecil Wright**, presidente di **Anssaif** (Associazione Specialisti di Sicurezza in Aziende di Intermediazione Finanziaria), in qualità di chairman ha puntualizzato alcune

premesse sul tema in questione: "Da una recente indagine condotta da Anssaif emerge come non solo l'utilizzo degli strumenti elettronici messi a disposizione delle banche sia assai contenuto, ma anche come l'informativa relativa alle misure di sicurezza venga percepita sia talvolta poco comprensibile all'utente finale. In particolare la fascia tra i 26 e 35, con titolo di studio di scuola superiore o laurea, è quella più insoddisfatta. Più in generale emerge una necessità diffusa di informazione e assistenza che sottolinea la necessità di ripristinare il rapporto umano cliente-banca".

### Serve più collaborazione

Secondo **Paolo Campobasso**, chief security officer di **UniCredit Group**, l'impegno sul fronte della sicurezza può costituire un elemento in grado di rafforzare la relazione in particolare tra il cliente impresa e la banca. "Quante imprese corporate sono correttamente strutturate al loro interno per rispondere alle sfide della sicurezza? E di conseguenza, quante aziende sono in grado di fornire un servizio di sicurezza efficace ai loro stessi clienti? Presso UniCredit è partita una riflessione che ci vede impegnati, in collaborazione con i colleghi della parte corporate, a definire un servizio dedicato alle aziende che fanno parte del nostro parco clienti teso a fornire suggerimenti per governare meglio la loro sicurezza fisica e logica, nonché le loro eventuali unità antifrode. La proposta di un servizio aggiuntivo rispetto all'offerta di altri gruppi può rappresen-





## Oltre 800 persone al Security Summit di Milano

Più di 800 persone hanno preso parte ai numerosi eventi di Security Summit, dal 24 al 26 marzo scorsi a Milano, che hanno permesso di scoprire le nuove frontiere dell'information security, un settore in continua evoluzione e in cui, come ha spiegato Steve Santorelli, ex membro dell'unità Computer Crime di Scotland Yard, la criminalità organizzata ha ormai rimpiazzato la figura dell'hacker solitario, diffusasi negli anni 80. E in cui le vecchie minacce, come virus, worm e firewall, si sono viste affiancare e superare da malware, botnet, cyberterrorismo: parole che sono ormai diventate indispensabili per capire l'evoluzione del settore. Il crimine informatico, oggi, vede in prima fila vere e proprie organizzazioni criminali che portano attacchi in grande scala contro cittadini, imprese e addirittura interi Stati. Questo spiega perché ormai gli attacchi che mirano ad abbattere la rete sono diventati sporadici: Internet è una fonte troppo importante di guadagni perché a qualcuno venga in mente di distruggerla. Il vero obiettivo è il profitto, ottenuto rubando le informazioni personali degli utenti, per poi utilizzarle sia direttamente, ad esempio per prelevare denaro dai conti correnti on line, sia come merce per il mercato nero dell'underground economy, dove nell'ottobre del 2008 si è toccato il picco di 30mila messaggi ogni ora.



## Il futuro del settore

Il problema della sicurezza informatica, hanno concordato i rappresentanti delle imprese leader nel settore, tra cui Cisco, Ibm, Oracle e Symantec, non sparirà: cambieranno le forme in cui vengono portati gli attacchi e i dispositivi attaccati, ma la criminalità informatica continuerà a crescere, perché lo spostamento delle attività economiche e sociali in rete aumenterà la possibilità di trarre profitti illeciti. Una prima sfida è nel breve termine, secondo le stime presentate da Mauro Orlando, associate director di Gartner Consulting: la crisi, infatti, da un lato restringerà i budget a disposizione dell'it, dall'altro costringerà le aziende a evitare passi falsi in materia di sicurezza, in quanto un incidente potrebbe causare un grave danno di immagine, aggravando le difficoltà del periodo economico. Un paradosso che potrebbe essere risolto spostando gli investimenti dall'hardware e dal personale verso le soluzioni software e l'outsourcing. Uno degli scenari possibili per il futuro è quello della sicurezza "as a service", in cui fornitori esterni offrono soluzioni di sicurezza standardizzate, permettendo di abbattere i costi di gestione interna e di rispondere più efficacemente, e in modo coordinato, alle nuove minacce. L'evoluzione della tecnologia e delle abitudini d'uso degli utenti, infatti, moltiplica le potenziali vulnerabilità e le opportunità di attacco: lo dimostra il caso della diffusione dei social network, accompagnata dalla comparsa dei primi worm basati su Facebook. Le applicazioni web, non a caso, sono la prima fonte di pericolo per le aziende e gli utenti privati, anche a causa della loro diffusione e del loro utilizzo nei social network.

Appuntamento al Security Summit di Roma - 10/11 giugno 2009

[www.securitysummit.it](http://www.securitysummit.it)

tare un forte elemento di fidelizzazione". Un altro aspetto del tema della sicurezza in banca sottolineato da Campobasso è quello della mancata condivisione delle best practice a livello di sistema. "Gli operatori devono ritrovarsi per lavorare insieme per prevenire e rimediare alle lacune dei sistemi di sicurezza. Solo in questo modo contribuiremo a rafforzare la fiducia del cliente finale e potremmo elevare il livello complessivo delle mi-

sure di protezione che in questo momento sono frammentate a livello di sistema".

### Educare il cliente finale

Vincenzo Giardina, responsabile funzione Audit Ict nell'ambito del Servizio Internal Audit del **Consorzio Operativo Gruppo Mps**, sottolinea come sia prioritario per il sistema bancario incrementare l'attività finalizzata a educare il

cliente sulle misure di sicurezza: "Il miglioramento dei livelli di sicurezza non passa solo attraverso l'evoluzione tecnologica in quanto tale, ma anche attraverso l'educazione del cliente finale, il quale deve essere stimolato a utilizzare i nuovi servizi sui canali on line perché non solo li conosce ma ne ha percepito in pieno l'utilità. Questa attività va però svolta a 360°, ovvero mettendo in atto una campagna che preveda la forma-



zione degli operatori all'interno della banca stessa. Solo in questo modo gli strumenti di accesso alla banca potranno essere proposti in modo corretto". Dello stessa opinione è **Leonardo Procopio**, consigliere **Ansaif** che invita a investigare meglio le caratteristiche di coloro che non utilizzano i nuovi device perché li percepiscono come poco sicuri. "Bisogna invitare a utilizzare in modo più consapevole questi strumenti anche incentivando le pratiche corrette per evitare le frodi elettroniche in generale. Non dimentichiamo che le frodi sono in generale un problema sociale perché minano i rapporti tra le persone e tra le persone e le aziende stesse andando a ostacolare le naturali dinamiche del credito".

#### Attenzione al linguaggio

**Paola Guerra Anfossi**, docente percorso criminalità e sicurezza presso l'**Università Cattolica del Sacro Cuore**, invita tuttavia a fare attenzione a quale tipo di informazioni possono essere utilmente veicolate al consumatore finale: "E' molto importante per il sistema bancario comprendere che la sicurezza non può essere comunicata in modo tecnico, ma deve essere comunicata con il linguaggio del target a cui è destinato il messaggio. Vi è ancora un'ampia fascia



di utenti che non ha fiducia negli strumenti che gli vengono proposti: emerge allora la necessità di fornire poche informazioni, purché siano chiare e serene". A portare il punto di vista di una grande banca straniera presente in Italia come **Bnp Paribas** sono **Anna Ryolo**, head of Organization, Bcp manager, e **Romain Defline**, Group Compliance, Group Business Continuity, che hanno ripreso

gli spunti lanciati da Paolo Campobasso. "Un'importante area destinata a crescere è quella della consulenza alle imprese sul fronte della sicurezza, afferma Ryolo. Abbiamo ad esempio potuto sperimentare direttamente che alcune istituzioni finanziarie ci hanno chiesto della consulenza sul tema della continuità operativa. Siamo stati pertanto visti non solo come fornitori di servizi critici e per questo obbligati ad avere un piano di continuità operatori ma anche come potenziali interlocutori per soddisfare i bisogni di sicurezza di altri operatori". La fiducia e la percezione della sicurezza, ha aggiunto Defline, non possono essere individuate in un tool bensì nella relazione costruita tra la banca e il cliente. "Il presupposto per usare il tool è la fiducia: altrimenti anche il tool può evoluto avrà fallito in parte il suo scopo. Oggi la sicurezza viene percepita come qualcosa di invasivo: spetta a chi fornisce il servizio far sì che tale percezione venga attenuata e sostituita con la valutazione dei benefici derivanti dall'uso delle nuove tecnologie".

R.B.

