

# Dopo il caso HSBC e quello tedesco

## Dati rubati, le banche corrono ai ripari

Parla il CEO di WiseKey, azienda leader nel settore della sicurezza dati

Venerdì la conferma che il Land tedesco del Nordreno-Vestfalia ha infine acquistato un dischetto contenente i dati bancari di 1.500 presunti evasori fiscali tedeschi con conti in Svizzera. Il costo della transazione si aggirerebbe attorno ai 3,7 milioni di franchi. Quasi contemporaneamente, il Baden-Württemberg ha invece deciso di rinunciare definitivamente a un'operazione analoga. A Berna ieri il Partito liberale radicale svizzero ha depositato un'interpellanza urgente per chiedere al Governo di denunciare la Germania presso la Corte internazionale dell'Aja per l'acquisto dei dati rubati. Sempre ieri è poi saltato il vertice a Berlino tra Hans-Rudolf Merz e Wolfgang Schäuble, a causa del ricovero in ospedale di quest'ultimo. L'incontro avrebbe dovuto preparare la ripresa delle discussioni sulla nuova Convenzione di doppia imposizione, con cui Merz spera di riuscire a frenare il preoccupante fenomeno del furto di dati. Berlino esamina attualmente la domanda di assistenza giudiziaria di Berna, che ha chiesto informazioni sui dati offerti su presunti evasori con conti in Svizzera. Ma è così facile rubare dati bancari di clienti di un qualunque istituto elvetico? Abbiamo interpellato in proposito Carlos Moreira, fondatore e CEO di WiseKey, società per la sicurezza informatica basata a Ginevra, che annovera tra i suoi clienti decine di banche, industrie e amministrazioni statali. Attiva in Svizzera da oltre un decennio, WiseKey s'appresta quest'anno ad essere quotata in borsa, confermando così d'essere una delle aziende leader nel settore.

PAGINA DI DAVIDE VIGNATI

### L'INTERVISTA

**Il furto di dati è un fenomeno con cui le banche elvetiche hanno sempre dovuto confrontarsi o si tratta di una problematica più recente - almeno in queste proporzioni - dovuta alla crescente pressione dei Governi esteri disposti ora ad addirittura acquistare informazioni rubate?**

«Direi che questo nuovo recente e preoccupante fenomeno dell'acquisto delle informazioni è andato a sovrapporsi al processo di informatizzazione e centralizzazione dei dati avviato dalle banche a partire dagli anni '90. Prima di allora, le banche avevano un sistema di gestione dei dati che definirei "dissociato", ovvero ogni consulente gestiva un proprio numero di clienti ed era direttamente responsabile per la sicurezza dei loro dossier e dei dati contenuti. Anche se la gestione dei dati era più "artigianale" rispetto alle possibilità offerte oggi dall'informatica, paradossalmente il livello di sicurezza era superiore. Ma con la progressiva informatizzazione del sistema, i dati sono stati via via stoccati in poche banche dati centralizzate, rendendo così più facile copiare e rubare in pochi istanti migliaia e migliaia di nomi di clienti e relativi dati bancari. E questo non riguarda solo le banche, lo stesso processo è avvenuto nell'industria o nelle amministrazioni statali. Per un decennio si è creduto che la centralizzazione dei dati fosse la maniera più razionale di gestirli, ma parallelamente non si è investito abbastanza nei sistemi di sicurezza».

**Ma è possibile con un sistema di sicurezza informatico dare una garanzia assoluta contro il furto o la manipolazione di dati, indipendentemente dal cosiddetto «fattore umano»? Quale soluzione proponete alla vostra clientela?**

«La sicurezza assoluta ovviamente non esiste, ma si possono minimizzare i rischi. Con i nuovi sistemi di sicurezza informatici a disposizione si può fare in modo che i dati bancari non siano mai depositati in alcun luogo, bensì smembrati e poi sparsi in più banche dati. Lo stesso nome del cliente non dovrebbe mai apparire integralmente da nessuna parte. I file di ogni cliente dovrebbero infatti poter essere letti solo decrittando i diversi pezzi e rimettendoli insieme. Solo attraverso delle chiavi biometriche, attivabili cioè con le impronte digitali, dovrebbe poi essere possibile decrittare e leggere questi file. E anche queste chiavi dovrebbero essere programmate e distribuite al-

l'interno dell'istituto bancario in base al grado d'accesso concesso ad ogni impiegato. In ultima analisi, solo i quadri e i membri della direzione dovrebbero poter disporre di chiavi biometriche in grado di leggere l'insieme dei dossier di tutta la clientela».

**Un tale sistema di sicurezza avrebbe potuto impedire il furto dei dati dalla filiale ginevrina della HSBC?**

«Sì, perché il caso HSBC non riguarda i sistemi di stoccaggio in quanto tali, che sono per lo più affidabili, come Oracle, Microsoft Access, D-base, etc, ma concerne invece la messa in sicurezza dell'accesso ai dati. I tecnici informatici dovrebbero avere accesso solo a certi dossier e unicamente previa autorizzazione dei direttori della sicurezza o dei direttori operativi, se non addirittura solo dei membri della direzione. In nessun caso dovrebbero poter assemblare e leggere i file completi della clientela. Inoltre, in caso di sospetto di lettura non autorizzata o di manipolazione dei dati, come fu il caso alla HSBC, dovrebbe essere possibile bloccare in maniera istantanea per via informatica o telefonica l'accesso a qualsiasi dato grazie a dei processi d'identificazione "forti", chiamati in gergo "Private Key Infrastructure", una sorta di ultima barriera contro ogni furto o utilizzo improprio di dati. Cosa che però le banche non sempre fanno».

**Ma se questi sistemi di sicurezza sono già disponibili, perché tutte le banche non ne fanno sistematicamente uso?**

«Le ragioni sono molteplici. Ma direi che per quanto riguarda la realtà elvetica, siamo in presenza di due estremi: da un lato le grandi banche preferiscono fare tutto per conto proprio, senza ricorrere a società specialistiche esterne, che hanno però il pregio di poter sviluppare e offrire sistemi di sicurezza sempre all'avanguardia. Così facendo, i grandi istituti accumulano sempre un certo ritardo, perché non impiegano abbastanza mezzi per la ricerca e lo sviluppo in proprio. Il fatto è che in Svizzera non esistono grandi società per la gestione della sicurezza informatica, per lo più esistono solo piccole e medie start-up che



Nelle banche elvetiche non è ancora diffuso il sistema delle chiavi biometriche e del controllo individuale d'accesso ai dati



però non offrono le necessarie garanzie in termini di capacità e continuità ai grandi istituti bancari, che dunque preferiscono fare in proprio. Differente è invece il caso delle piccole banche private o di quelle cantonali, che preferiscono invece dare in "outsourcing" tutta la gestione dell'informatica, ivi compresa la sicurezza, col rischio che siano appunto degli esterni a gestire questi sistemi di controllo d'accesso ai dati, che non sono dunque direttamente gestiti e controllati dai quadri dell'istituto bancario. Così facendo l'intero sistema è meno efficiente e rapido».

**La clientela ha dunque delle ragioni valide per dubitare dell'affidabilità dei sistemi di sicurezza adottati dalle banche elvetiche?**

«Sì e no. La Svizzera resta uno dei Paesi più sicuri al mondo in materia di sicurezza dei dati, ma resta il fatto che non vi sono degli standard uniformi e che il grado di sicurezza può variare molto da istituto a istituto. Aggiungerei però che quanto sta avvenendo, dal caso Liechtenstein a quello della HSBC, fino alle liste rubate e in vendita in Germania, ha riproposto in modo forte il problema della sicurezza informatica e quasi tutte le banche elvetiche stanno ora procedendo ad un riassetto dei propri sistemi».

**Le banche elvetiche stanno dunque correndo ai ripari?**

«Direi di sì. Si sta procedendo all'introduzione sistematica dell'identificazione biometrica per tutti i collaboratori. Si sta dunque applicando la cosiddetta nozione di controllo dell'"accesso" per minimizzare il più possibile i rischi. Naturalmente non tutti si stanno muovendo alla stessa maniera. Stando a quanto ci dicono i nostri clienti e alle sollecitazioni che stiamo ricevendo, c'è ancora una certa confusione su quale direzione prendere e gli investimenti da fare. Direi che il caso HSBC, per la quantità enorme dei dati rubati, ha creato un certo panico tra molti istituti bancari. Se mi consente una metafora, è come se si fosse appena schiantato un aereo, e ora

tutti si domandano se la colpa sia stata solo del pilota, o di un guasto tecnico al velivolo o semplicemente delle condizioni atmosferiche... e tutti sono alla ricerca della scatola nera per stabilire che cosa nel sistema non abbia funzionato correttamente».

**Ma sul piano internazionale, ritiene che gli istituti elveticchi abbiano accumulato un ritardo dal punto di vista della sicurezza dei dati rispetto a quelli di altri Paesi?**

«Rispetto al Nordamerica sicuramente, anche se naturalmente le sollecitazioni a cui è sottoposta in questo momento la piazza finanziaria elvetica è unica e credo dunque che sia difficile fare paragoni. Negli Stati Uniti, comunque, se penso al sistema di decriptazione sviluppato ad esempio da Citigroup, direi che sono più all'avanguardia rispetto ai grandi istituti elveticchi. D'altronde non è una sorpresa, in ambito informatico gli americani sono sempre stati in anticipo sull'Europa. Ma al di là dello sviluppo dei sistemi informatici di stoccaggio ed accesso ai dati, gli Stati Uniti hanno anche già sviluppato da tempo degli standard di sicurezza codificati e uniformati, al fine di creare una sorta di "certificato" nazionale per spingere i principali istituti a mettersi al passo coi sistemi di sicurezza più avanzati. Questo anche con lo scopo di mettersi al riparo da ogni possibile causa giudiziaria per negligenza in caso di furto o manipolazione dei dati».

**Come funziona questo «certificato di sicurezza» adottato negli Stati Uniti?**

«Si chiama "Indentrus.com" ed è un partenariato pubblico-privato che permette di gestire efficacemente i rischi associati all'autenticazione dell'identità bancaria negli Stati Uniti. Si tratta cioè di un'associazione pubblica che fissa e certifica a livello nazionale gli standard e i principi di sicurezza che le banche devono mettere in atto. È una sorta di ISO 9000 per la sicurezza bancaria, che regola anche nei dettagli i sistemi di accesso ai dati da parte di tutti i collaboratori. Il rispetto di tali standard va poi riconfermato periodicamente».

**Ritiene che un simile sistema di certificazione pubblico-privato possa migliorare la sicurezza dei dati bancari anche in Svizzera?**

«Ne sono persuaso. È questione di tempo, ma prima o poi vi dovremo arrivare anche noi. In Svizzera oggi ogni banca ha un suo sistema di sicurezza e convivono l'uno accanto all'altro standard tra loro molto diversi. E come ha mostrato il caso HSBC, basta la falla in un solo istituto per macchiare la reputazione dell'intera piazza finanziaria a livello internazionale. Ma non sarà facile, serviranno delle riforme politiche, perché le nostre banche non sono pronte a condividere un sistema nazionale di certificazione della loro sicurezza interna».

**Cosa hanno da perdere?**

«Non piace l'idea di demandare ad un organo di controllo esterno la verifica dei propri sistemi di sicurezza, tanto più se quest'organo è partecipato dalla concorrenza, col rischio poi magari che il "ranking" degli istituti più e meno sicuri sia reso pubblico. Né l'Associazione svizzera dei banchieri, né la Banca nazionale, né tanto meno i più importanti attori della nostra piazza finanziaria sembrano per il momento interessati a collaborare per tentare una riforma in questo senso. La sicurezza e la fiducia sono due cose distinte. Gli istituti bancari americani e anche quelli di Singapore lo hanno compreso e collaborano già da tempo tra loro per garantire standard comuni di sicurezza in funzione della competitività con le piazze finanziarie estere. Se la Svizzera non colmerà questo ritardo, continuerà a perdere terreno nei confronti della concorrenza mondiale nel campo della protezione tecnologica della sfera privata. Questi continui furti di dati rischiano infatti di arrecare alla piazza elvetica altrettanti danni che le continue pressioni sul segreto bancario».

**Ma con il sistema «Melani», la Svizzera ha già comunque creato un ente federale per la protezione delle banche da attacchi informatici esterni.**

Vi sono troppe disparità di standard di sicurezza da una banca all'altra. Serve una certificazione nazionale come negli USA

### COLMARE IL RITARDO

Secondo Carlos Moreira, fondatore e CEO di WiseKey, l'avvenire della piazza finanziaria elvetica passa necessariamente per una maggiore sicurezza nella protezione dei dati bancari. Il caso HSBC ed il furto di informazioni relative a presunti evasori tedeschi con conti in Svizzera hanno spinto numerosi istituti elveticchi a rivedere i propri sistemi di controllo.

**Potrebbe essere questo un punto di partenza?**

«Potrebbe, anche se Melani si basa su una vecchia visione di sicurezza, l'attacco informatico esterno appunto, che non ha richiesto alle banche una compartecipazione dei controlli dei rispettivi sistemi di sicurezza interni. Fin dall'inizio dell'informatizzazione delle banche negli anni '90, gli hacker hanno sviluppato una metodologia scientifica per individuare le loro falle di sicurezza. Melani serve a questo, ma si basa sulla "strategia del ridotto", dell'attacco esterno, mentre oggi siamo alle prese con una minaccia ben più infida, quella dall'interno».

**Come bisognerebbe dunque procedere?**

«Bisognerebbe cominciare con l'istituire a livello federale una commissione di esperti, che possa analizzare i sistemi di sicurezza interni di tutte le banche, e a partire da questa analisi formulare delle norme di sicurezza standard a cui tutte le banche dovrebbero uniformarsi per potere esercitare la loro attività in Svizzera. È importante che il risultato di questa operazione sia visibile, ovvero che le banche che ottengono il certificato di garanzia di sicurezza possano esibirlo per la propria clientela. Questo incentiverebbe le banche a fare i necessari investimenti per mettersi al pari coi nuovi standard. A un organo indipendente dovrà poi essere demandata l'autorità di verificare con regolarità il rispetto degli standard per poter continuare a fregiarsi del certificato. La Svizzera ha interesse a sviluppare un simile sistema di sicurezza condivisa e certificata, soprattutto sapendo di essere ormai un obiettivo prioritario di questi ripetuti furti di dati. La nostra piazza finanziaria dovrebbe dunque investire subito in queste nuove tecnologie di sicurezza, affinché questo aspetto possa divenire un nuovo "atout" che gli istituti elveticchi poranno far valere nei confronti della concorrenza internazionale. Tanto più oggi, che l'indebolimento del segreto bancario richiede alla piazza elvetica di reinventarsi e profilarsi meglio per la capacità e la professionalità di gestione dei patrimoni, come pure per la stabilità e la sicurezza del nostro sistema».