

SICUREZZA NEI SERVIZI BANCARI

*un problema reale
per il mondo virtuale*

a cura di

MARCO BURATTI e MARCO TEMPRA

Il tema della sicurezza è molto caro al settore bancario, il quale, nel corso dei secoli, con un processo di continuo aggiornamento al mutare degli scenari e del contesto in cui opera, ha affinato accorgimenti sofisticati per tutelare e proteggere i beni materiali ed immateriali ad esso affidati.

Un tema, quello della sicurezza, che subito richiama alla mente oggetti tangibili quali la cassaforte, il caveau, le inferriate ed i vetri corazzati, che fanno parte del nostro vissuto o comunque dell'immaginario collettivo. Tutti elementi molto concreti, a volte anche un poco fastidiosi, come le porte girevoli all'ingresso delle filiali.

In realtà, le banche hanno messo in atto un sistema integrato di strategie rivolte a risolvere differenti problematiche inerenti, per esempio:

- la sicurezza fisica (quella più evidente, della quale abbiamo appena dato qualche esempio);
- la sicurezza dei sistemi informativi, delle applicazioni informatiche e dei dati;
- gli aspetti organizzativi, normativi, di controllo;
- l'individuazione di nuovi prodotti e soluzioni che limitino i rischi connessi alla gestione del denaro, come ad esempio le carte di pagamento che limitano il contante in circolazione.

Le minacce fino a qualche decina di anni fa erano tipicamente di tipo fisico ed organizzativo: si trattava di difendere il perimetro della banca, di proteggere con la cassaforte i valori posseduti, di porre in atto strumenti di controllo e modalità di lavoro che impedissero lo svolgimento di attività non coerenti con le finalità aziendali.

La diffusione dell'informatica, a partire dagli anni '70, ha introdotto nuove problematiche di sicurezza logica, le-

gate cioè alla integrità, affidabilità e segretezza dei dati trattati. In questo caso le strategie adottate riguardano la gestione dei sistemi informatici, la continuità di servizio degli apparati e delle procedure, il corretto funzionamento dei programmi, la predisposizione di infrastrutture ridondate (cioè con più elementi in grado di svolgere lo stesso lavoro) che possano garantire il funzionamento anche in caso di guasto di una componente del sistema.

Il recente avvento delle nuove tecnologie legate al mondo Internet, sebbene abbia migliorato la vita di tutti i giorni, ha reso nuovamente inevitabile il confronto con i rischi indotti dalla tecnologia. Le nuove tecnologie, potenti ed efficaci, in grado di mettere in relazione le controparti ovunque esse si trovino ed in qualsiasi momento, sono una grandissima opportunità di miglioramento del livello di servizio offerto alla clientela, la quale trova ormai più che normale l'utilizzo dei servizi online e della Rete in genere.

Purtroppo, come nel mondo "fisico", anche sulla Rete si muovono dei malintenzionati che cercano il loro profitto con azioni illecite. Niente di nuovo sotto il sole, anche se in un nuovo contesto.

SECURITY IN BANKING SERVICES, A REAL PROBLEM FOR THE ONLINE WORLD

The bank is the guardian of the valuables entrusted to it. But this task has developed on different aspects. It no longer regards protecting physical valuables with security systems. Nowadays, security systems also have to protect computer systems and data that clients use. In addition, solutions have to be found that reduce the risks connected to the management of on-line accounts. Internet is the special area where this battle is being fought. No one can realistically think of giving up current transactions in real time. But the fact is that hackers' sophisticated inventions to winkle out a User ID, Password or codes are on the increase. An excellent method in this respect is 'Phishing' whereby Web pages can be created that simulate official communications.

Le banche sono, ovviamente, in prima fila per combattere il fenomeno, considerando che utilizzano i canali remoti (*in primis* Internet) per poter erogare servizi personalizzati e disponibili 24 ore al giorno.

Si sono quindi trovate a trasferire su Internet (o meglio ai loro clienti dei servizi online) quella profonda cultura della sicurezza che già le caratterizza nel mondo reale. Ciò ha portato, come già succedeva da secoli nel mondo fisico, alla costruzione di fortezze e cassaforti, questa volta informatiche, continuamente aggiornate per resistere ai potenziali attacchi dei malviventi. Accorgimenti organizzativi, associati a tecnologie sofisticate sottendono alla segretezza e all'affidabilità dei dati e dei programmi, a tutela e garanzia della serenità dei propri clienti che possono godere in tutta sicurezza della grande comodità della banca virtuale.

Tuttavia è necessario che l'utilizzatore della Rete, il Cliente, ponga attenzione a come opera su Internet, contribuendo, con piccoli accorgimenti ed abitudini, ad innalzare ulteriormente il livello di sicurezza complessiva del sistema.

Se fino a pochi mesi fa lo spauracchio per chi navigava nella Rete era riferito a termini come *virus* o *worm*, oggi ormai i rischi maggiori derivano dalla perdita/furto di informazioni o dalla cosiddetta sostituzione di identità personale.

Gli aggressori, i rapinatori del terzo millennio, hanno individuato nell'utilizzatore dei servizi il "tallone di Achille" del sistema. Perché affaticarsi con scarse possibilità di successo e molti rischi nel tentare di superare le potenti difese messe in atto dalle aziende di credito a supporto dei propri sistemi informativi quando, con poco sforzo, è possibile farsi consegnare da un cliente distratto le "chiavi" per l'accesso? È vero che così facendo il malvivente avrà accesso esclusivamente alle funzioni e alle informazioni di quella determinata persona, ma potrebbe essergli sufficiente poter replicare la frode su un buon numero di individui per raggiungere il proprio obiettivo.

Per questo motivo occorre prestare le dovute cautele, quando ci si muove nella Rete, alla stessa stregua di quanto facciamo nel mondo fisico, e come non consiglieremmo le chiavi di casa ad un emérito sconosciuto, così dobbiamo porre attenzione nel non consegnargli, magari

LINEE GUIDA ABI

La "Centrale di allarme per attacchi informatici" dell'ABI (Associazione Bancaria Italiana) ha stilato norme di comportamento per i clienti.

Vi riportiamo le principali linee guida:

1. diffidare dalle richieste, giunte via e-mail, per l'inserimento di dati riservati (le banche non chiedono queste informazioni per posta elettronica);
2. non cliccare sui link presenti in e-mail sospette specie se fanno uso di toni "intimidatori";
3. diffidare delle e-mail con indirizzi web molto lunghi con caratteri inusuali;
4. verificare al momento dell'accesso ai siti di Internet Banking che la pagina sia protetta (protocollo *https* e sia riportato, usualmente, nell'angolo in basso a destra un lucchetto chiuso);
5. porre particolare attenzione all'inserimento dei codici di accesso all'Internet Banking in pagine pop-up;
6. aggiornare spesso i browser per l'accesso ad Internet;
7. avvisare la banca di situazioni sospette che rientrino nelle fattispecie elencate.

senza rendercene conto, il Codice Utente e la Password di un servizio online.

Una delle minacce più frequenti (che può colpire anche nel mondo reale) consiste nel fenomeno del *Social Engineering* che prevede una serie di "attacchi" per raccogliere *User ID* e *Password* o numeri riservati direttamente dagli utilizzatori sfruttando le vulnerabilità più elementari degli utenti che si lasciano aggirare con false telefonate, con intercettazioni telefoniche, *phishing*, ecc.

La comodità, l'efficacia e il valore economico dei servizi online sono talmente alti che l'ipotesi di rinunciare al "virtuale" è assolutamente improponibile (pensiamo a quanto stanno investendo sull'*egovernment* tutti i Paesi più avanzati, considerando l'efficienza indotta dalle nuove tecnologie un fattore strategico per la loro competitività, oppure a come sta crescendo il fenomeno dell'*ecommerce*, che propone nuovi modelli e modalità di acquisto a tutto vantaggio dei compratori). E poi spesso il modo "fisico" è meno sicuro del virtuale: quante volte, ad esempio, avete consegnato la vostra carta di credito al cameriere, quando invece utilizzandola su Internet avete a disposizione strumenti sofisticati per proteggerla? Quante volte, pagando col bancomat o la carta di credito, avete ridotto la carta moneta circolante e quindi la possibilità di furto ed aggressioni?

Il consiglio è quello di continuare ad usufruire dei grandi vantaggi offerti dal mondo "virtuale" mettendo però in atto alcune elementari precauzioni che dovrebbero divenire parte delle nostre abitudini. Di seguito, per Vostra utilità, riportiamo alcuni suggerimenti stilati dall'Associazione Bancaria Italiana. Nello specchietto a lato trovate anche una descrizione della tecnica del *phishing*, utile per comprendere appieno il senso di tali suggerimenti.

Per una maggiore tranquillità è bene farsi aiutare da tecnologie "buone", come un filtro *antispam* che intercetti i tentativi di *phishing* più noti prima che possano raggiungere la casella di posta, così come ad un *antivirus* aggiornato.

Il phishing

Il *phishing* è una minaccia in agguato per chi naviga su Internet, basato sulla creazione di pagine web ideate per simulare comunicazioni ufficiali da parte di un'azienda, di un'istituzione bancaria, di un ente che si intende attaccare.

Lo scopo è quello di aggirare gli utenti Internet per ottenere informazioni personali e riservate quali la *User ID* e la *password* per accedere ai servizi di Internet Banking o acquisire gli estremi delle carte di credito.

Falsi messaggi, in genere inviati per posta elettronica, inducono i destinatari a collegarsi, per esempio, al sito della propria banca. I messaggi, di norma, sono studiati in modo tale da indurre una certa fretta e invitano a recarsi immediatamente sul sito per qualcosa di importante (ad esempio: «La invitiamo a collegarsi al più presto al sito antifrode della sua banca, il cui indirizzo è di seguito riportato, ove troverà una importante comunicazione che La riguarda»). L'indirizzo riportato nel messaggio punta ad un sito del tutto simile nella grafica a quello reale, ma purtroppo si tratterà di un sito falso, "clonato", che inviterà il malcapitato ad inserire i propri codici identificativi, credenziali di accesso o numeri di carta di credito. A questo punto il sito fornirà una qualsiasi risposta credibile e lascerà il Cliente del tutto tranquillo. Il malvivente avrà così ottenuto gli elementi utili a collegarsi al vero sito dell'azienda aggredita.

La tecnica del *phishing* può essere utilizzata attraverso uno *spamming*, cioè un invio massivo a caselle di posta elettronica "raccattate" con ogni

La risposta di BPS



SCRIGNOcard è la tessera, strettamente personale, che consente di autenticarsi e accedere, in modo sicuro, ai servizi di **SCRIGNObps**. La **SCRIGNOcard** si adegua al mutato contesto ambientale rispondendo all'aumentato livello di sicurezza richiesto a un sistema di Internet Banking, ma anche all'opportunità di essere impiegata, come unico strumento di autenticazione, su tutti i canali di comunicazione con la banca che, via via, verranno resi idonei alla fruizione di **SCRIGNObps**.

Il cliente gode di un elevato livello di sicurezza: oltre ad immettere il Codice Utente e il PIN, costituito da 5 cifre, si autentica ai servizi online inserendo ulteriori due codici che si trovano nella griglia – una specie di tabella a due entrate un po' simile a quella che si utilizza quando si gioca a "Battaglia navale" – presente sul retro della **SCRIGNOcard**.

Ad ogni collegamento vengono richieste coordinate scelte in modo casuale; pertanto, i codici numerici da inserire, individuati sulla base di tali coordinate, saranno diversi di volta in volta.

mezzo. Non è detto che tutti i destinatari siano davvero clienti dell'azienda aggredita, ma in questo caso probabilmente ignoreranno il messaggio. C'è però la probabilità, tanto più alta quanto più "importante" è la base di clienti dell'azienda aggredita, che alcuni dei destinatari siano effettivamente utilizzatori del sito citato nel messaggio. Sui grandi numeri, basta una piccola percentuale di casi positivi per far felice il furfante.

Secondo stime dell'associazione *anti-phishing* (www.antiphishing.org), quasi il 5% di coloro che ricevono i messaggi è indotto psicologicamente a rispondere. Da qui la grande attenzione delle istituzioni (ABI, Co.Ge.Ban., Pubblica Sicurezza, ...) al problema e le conseguenti reazioni di soggetti interessati come le banche. ■