Il commercio elettronico si diffonde anche in Italia

Faccio la spesa al "cybermercato"

di Alberto Robiati

Nel '99 gli acquisti on-line in Italia hanno "mosso" 400mila miliardi di lire ("solo" 100 nel '98). Ma è ancora forte la diffidenza verso le modalità di pagamento, la riservatezza dei dati e la qualità della merce

Un... acquirente all'opera

Sito di un "cybermercato" qualsiasi. C'è la pagina dei libri, quella delle ultime uscite discografiche, dei cd-rom multimediali. Si trova facilmente la T-shirt alla moda, un Pc della prossima generazione, una vantaggiosissima offerta di viaggio. Il click cade su uno di quei prodotti introvabili qui da noi. Il nostro alter ego virtuale colloca la merce nel carrello, altrettanto virtuale. Ancora un breve tour tra gli scaffali, più che mai virtuali, ed eccoci alla cassa. Virtuale anche questa, ma non le monete che ci richiede.

Siamo a un bivio: paghiamo con la carta di credito, digitando diligentemente il numero e scegliendo l'opzione "invia", o ci dileguiamo nascondendoci nel Web, ma gettando così all'aria minuti di shopping telematico e con essi il contenuto tanto desiderato del carrello? Essì, perché c'è poco da fidarsi: posso anche scrivere il numero della mia credit card ma chi mi assicura che non vedrò il mio conto prosciugato? Questo è il timore più diffuso fra utenti della rete che prima o dopo hanno scelto di acquistare via Internet.

E non è l'unico freno allo sviluppo italiano del commercio elettronico (o "e-commerce"). Un altro fattore critico riguarda la percezione, da parte di imprese e consumatori, del rapporto costi/benefici dell'uso commerciale del Web. Non c'è ancora una conclamata consapevolezza dei vantaggi offerti dal commercio virtuale che, dal punto di vista dell'azienda, riguardano la possibilità di espansione dei mercati, le basse barriere all'entrata, i costi ridotti. In favore di queste strategie si è espresso il congresso del Wto (l'Organizzazione mondiale per il commercio) nel quale è stato deciso di non tassare le transazioni elettroniche (per il momento...).

La prospettiva del consumatore può concernere invece la comodità, i prezzi vantaggiosi, la scarsa reperibilità di un dato prodotto. E' anche vero che la tipica mentalità italiana di "toccare con mano" gioca contro l'e-commerce, ma le vendite per posta dimostrano che lo scetticismo iniziale può essere superato.

IL NUMERO DI CARTA (O DI CONTO) SI PUO' PROTEGGERE

Questione centrale però resta la sicurezza. L'utente esperto sa che da diverso tempo esistono applicazioni in grado di proteggere lo scambio di dati riservati (ad esempio il numero di un conto corrente o quello di una carta di credito). Funzionano con algoritmi di crittografia che criptano i pacchetti di informazione in transito sulla rete.

Sono diverse le tipologie di problemi riguardanti la sicurezza: alcune informazioni possono essere intercettate e spiate da terze parti e quindi modificate (esempio cifre di conti correnti, bilanci, ecc.); l'identità di un utente può essere assunta da altri per effettuare operazioni economiche; l'imprenditore non può dimostrare l'autenticità del cliente.

La soluzione sicura è stata individuata da CommerceNet, un'organizzazione non-profit fondata per lo sviluppo del commercio elettronico via Internet. Perché una transazione in rete vada a buon fine devono essere garantite: la riservatezza dei dati, l'autenticazione delle parti (entrambe devono poter essere sicure dell'identità dell'interlocutore), l'integrità del messaggio (quello inviato deve essere identico a quello ricevuto), l'irrefutabilità della fonte (il mittente non può negare di aver inviato il messaggio) e della destinazione (il destinatario non può negare di aver ricevuto). Tutti questi punti vengono risolti mediante la crittografia che consente anche di produrre certificati e firme elettroniche. ▸

SODDISFATTI O RIMBORSATI

La legge italiana ha equiparato il commercio elettronico alla vendita per corrispondenza (a tutela dei consumatori vige la regole del "soddisfatti o rimborsati"). Ma l'e-commerce si differenzia da quest'ultima per le modalità di pagamento. Accantonato il vecchio contrassegno, l'utente della rete salda i suoi conti attraverso tre vie. La prima è simile al tradizionale pagamento con assegno (ma il trasferimento di fondi in questo caso avviene in tempo reale). Una seconda corrisponde a una sorta di denaro contante elettronico (il digital-cash), che può assumere diverse forme (ad esempio le carte prepagate o smart card, funzionanti con il meccanismo attuale delle schede telefoniche). Infine, l'e-cash. Le banche consentono la possibilità di spostamenti monetari sui conti dei contraenti quando entrambe le parti sono clienti delle stesse.

LA CHIAVE DELLA SICUREZZA

L'equivalente immateriale di una cassaforte è la crittografia che, nella società dell'informazione, sostituisce ogni serratura, lucchetto o cassetta di sicurezza.

Il sistema di cifratura più diffuso e più sicuro si basa sulla doppia chiave (una privata e una pubblica) per ogni utente. Il messaggio viene criptato con la chiave pubblica del destinatario, e solo chi possiede la corrispondente chiave privata è in grado di decifrarlo.

Il modello è sicuro, ma non matematicamente inviolabile. L'attacco più semplice è quello portato, come si dice in gergo, "con la forza", ovvero provando in sequenza tutte le combinazioni possibili sino a quando si indovina quella giusta. Con la chiave di 128 bit (vale a dire una catena di 0 e di 1 ripetuti per 128 volte) il tempo necessario per tale ricerca è virtualmente infinito. Una chiave di 40 bit, invece, è largamente sufficiente per fronteggiare gli attacchi di un utente molto esperto, ma può essere scoperta da centri di ricerca di altissimo livello (trovata dopo otto giorni ininterrotti di calcolo con l'utilizzo di un numero notevole di sistemi matematici). Infatti una sequenza di 40 bit origina un totale di 2exp40 combinazioni possibili, mentre per i 128 bit ve ne sono 2exp128 (la base è 2 perché due sono i numeri, cioè 0 e 1).

LE TECNICHE DI CIFRATURA FANNO LA DIFFERENZA

Sulla disponibilità, distribuzione e utilizzo della crittografia, è in corso un dibattito a livello mondiale, poiché possedere tecniche di cifratura particolarmente robuste può costituire un vantaggio competitivo per alcuni Paesi. La difficoltà maggiore è pertanto l'impossibilità di proporre un sistema standard valido per tutti. Ad esempio, negli Stati Uniti la legge vieta la vendita all'estero di algoritmi particolarmente complessi (quelli a 128 bit e oltre), utilizzati solo in campo militare; è inoltre illegale la crittografia che usa algoritmi non decifrabili dalla autorità governative (Cia, Fbi). In particolare il governo Usa identifica sette Paesi considerati a "rischio terrorismo".

Per questi motivi, le versioni d'oltreoceano dei software che usano la crittografia non possono essere distribuite in Europa e nel resto del mondo. E' il caso di Netscape, il cui protocollo di sicurezza Ssl è basato su chiavi a 128 bit negli Usa, e a 40 in Europa (di recente la "concessione" di Clinton porta le chiavi a 64 bit). Naturalmente sono in circolazione versioni europee con chiavi da 128, ma è bene assicurarsene. □

La Fiat Barchetta è offerta in internet