PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 333 di giovedì 10 maggio 2001

Accessi sicuri alle reti informatiche

Per proteggere i sistemi informatici da accessi non autorizzati non e' sufficiente una password. I mezzi piu' avanzati per ottenere un'autenticazione sicura.

Proteggere i sistemi informatici da accessi non autorizzati costituisce una priorita' per ogni azienda e, nell'ambito delle applicazioni di e-business, e' un'esigenza vitale.
La semplice adozione di una password non e' in grado di fornire la sicurezza che chi accede a dati strategici sia autorizzato a farlo.

Per questo motivo nuovi metodi di autenticazione degli utenti sono utilizzati per garantire la sicurezza dell'accesso ai dati.
Un approccio sempre piu' utilizzato e' quello dell'autenticazione a doppio fattore (Two factor authentication) che si basa sul riconoscimento combinato di due dati.

Molto diffusi sono i token hardware, simili a chiavi, prodotti hardware che sono applicati ai sistemi da proteggere: l'utente sara' identificato tramite la digitazione di un PIN (Personal Identification Number) e mediante l'oggetto posseduto dall'utente stesso.
Il sistema dei token hardware si basa su una generazione casuale di codici di accesso legati ad alcuni fattori (data e ora) e possono essere utilizzati per accedere ai dati da qualsiasi postazione.
Questo tipo di prodotto supera la limitazione delle smartcard, sulle quali sono memorizzati i dati dell'utente, che richiedono invece un apposito lettore collegato alla macchina utilizzata.

Un altro tipo di sistema per una identificazione sicura e' l'utilizzo di dispositivi, di difficile duplicazione, gestiti da un apposito lettore o da uno specifico ingresso del PC utilizzato per la connessione, quale ad esempio le porte USB (Universal Serial Bus).
Le chiavi USB non richiedono uno specifico lettore, ma possono interagire con le porte utilizzate dai recenti computer.

Infine tra i sistemi piu' avanzati compaiono i sistemi biometrici che si basano sul riconoscimento di inalterabili caratteristiche fisiologiche o comportamentali dell'utente (retina, iride, impronta digitale, voce).
I dati acquisiti tramite un lettore vengono confrontati con quelli contenuti in un data base.
Nell'applicazione dei sistemi biometrici non bisogna pero' tralasciare le questioni inerenti alla privacy e dei costi; per ottenere un grado di sicurezza elevata i costi da sostenere non sono indifferenti.
