Temi: Accesso ai dati
Categoria professionale: Direzione dei sistemi di sicurezza
Tipologia di dati: Privati

Come posso proteggere i dati dei clienti ?

Un partito politico ha affidato la gestione della sua informatica a una società privata.
La banca dati è stata piratata e i deputati hanno ricevuto dei messaggi sul cellulare e delle e-mail d'insulti.
I pirati hanno usato un' iniezione SQL, scoperta per caso utilizzando un motore di ricerca che ha permesso loro l'accesso a 160 banche dati legate al partito avendo il subappaltatore lasciato aperto il suo server MySql e utilizzato ovunque la stessa password.
Una società privata di protezione informatica che realizza una sorveglianza delle comunicazioni pubbliche tra pirati, ha scoperto l'avvenuto pirataggio di dati grazie a questo sistema.
Non si è mai troppo prudenti, soprattutto quando si subappalta il proprio sistema informatico. È sempre buona norma verificare le condizioni di sicurezza offerte dalla società privata.

Raccomandazioni
Il partito ha subappaltato a una società hosting senza definire una politica di sicurezza. E il detentore della collezione di dati a essere responsabile del trattamento dei dati che raccoglie direttamente o in subappalto. Il detentore della collezione di dati è responsabile dei dati che tratta. Deve regolarmente valutare le misure di sicurezza prese tenendo conto dei rischi riguardanti la protezione dei dati.

Prinicipi di base
Sicurezza dei dati

Esempio concreto
http://www.rue89.com/2011/11/08/les-donnees-personnelles-dun-millier-de-cadres-ump-piratees-226342