Thèmes : Accès aux données
Métiers: Direction des systèmes d'information
Types de données: Privées

Comment puis-je protéger les données des clients ?

Un parti politique a confié la gestion de son informatique à une société privée.
Les bases de données ont été piratées et les députés ont reçus des textos et des courriels d'insultes.
Les pirates ont utilisés une injection SQL, découverte par hasard en utilisant un moteur de recherche, ce qui leur a permis d'accéder à 160 bases de données en lien avec le parti, le sous-traitant ayant laissé quasi-ouvert son serveur MySql et utilisé le même mot de passe partout.
Une société privée de veille informatique, qui réalise une surveillance des communications publiques entre pirates, a découvert le piratage grâce aux robots qu'elle met en ligne.
On n'est jamais trop prudent, surtout si l'on sous-traite son système informatique. Il est prudent de vérifier les conditions de sécurité offertes par la société privée.

Recommandations
Le parti a sous-traité à une société d'hébergement sans définir de politique de sécurité. Or c'est le maître du fichier qui est responsable du traitement des données qu'il effectue directement ou en sous-traitance. Le maître du ficher est responsable de la sécurité des données qu'il traite. Il doit régulièrement évaluer les mesures de sécurité prises en tenant compte des risques en matière de protection des données.

Principes de base
Sécurité des données

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