Affaire Master Card: compléments d'informations

-Des informations qui n'avaient pas lieu d'être John M. Perry, PDG de CardSystems Solutions, a récemment confié au New York Times que « les informations volées étaient stockées à des fins de recherche et d'analyse». Cependant, la légitimité et la légalité de la base de données est véritablement remise en question depuis le début de l'enquête. La société CardSystems Solutions devait uniquement assurer le transit de la base de données et ne devait en aucun cas la stocker. Celle-ci contenait les noms de 40 millions de clients, les numéros de cartes de crédit ainsi que les codes de sécurité mais en aucun cas les adresses des usagers. **-70.000 français exposés** La presse se fait l'écho de chiffres tout à fait vertigineux, cependant la réalité semble tout autre. Il est certain que 200.000 numéros de cartes, parmi les 40 millions qui étaient à disposition, ont été exportés. En détail, il s'agit de 100.000 numéros Visa, 68.000 Mastercard et 30.000 provenant d'autres organismes. 70.000 numéros appartiendraient à des Français. **-Un manquements manifeste aux règles de sécurité** Visa et Mastercard ont conjointement développé un standard en matière de sécurité afin de prévenir la fraude et le piratage de leurs systèmes d'information. Ce standard doit être respecté par tout commerce de gestion de cartes de crédit. D'après Mme Jones, porte-parole de Visa, Cardsystems Solutions a bien été certifié en juin 2004 et tout était aux normes en matière de sécurité. Or, une évaluation « post-incident » conclue que ce n'est plus le cas et les manquement aux règles de sécurité ont coûté très cher à l'entreprise. **-Une faille IIS en cause ?** Peu d'informations circulent à propos de la ou les failles que le pirate aurait utilisées pour commettre son braquage virtuel. Cependant un récent communiqué de presse émis par la société eEye laisse entrevoir un début de réponse. En effet, la firme américaine vient de déployer en urgence leur produit « SecureIIS » chez CardSystems Solutions. Un serveur Web Microsoft IIS non « patché » serait donc le fautif ? **Olivier Devaux** pour **pour Vulnerabilite.com**