

Panic chez Panix: le FAI piraté

La page principale de Panix.com fournit une description détaillée de l'incident. La société australienne MelbourneIT, en charge de l'administration de la zone, n'aurait pas effectué un contrôle de routine alors qu'elle recevait un e-mail frauduleux demandant un transfert de l'autorité sur la zone. Une demande de confirmation aurait alors dû se faire auprès de l'administrateur de Panix. La zone s'est vu transférée d'abord vers une société britannique, puis vers une organisation canadienne, avant de revenir sous le contrôle du fournisseur de services. L'incident étant survenu durant le week-end, la remise en disponibilité de la zone n'a pu se faire que le lundi matin, heure de Melbourne. De plus, les mécanismes liés à la propagation des informations de zone n'ont pu rétablir le bon fonctionnement global que le jour suivant. C'est sans doute le premier incident du genre qui a paralysé l'ensemble des services d'un ISP pendant plus de 72 heures. Le tout basé sur l'exploitation de techniques de social engineering... (*)

pour Vulnerabilite.com