# Petit florilège de fraudes internes

- Informatique - Sécurité Informatique -

Date de mise en ligne : dimanche 26 avril 2009

## Les chercheurs de l'université de Carnegie Mellon / CERT US livrent quelques exemples de fraude interne issus d'une enquête méticuleuse sur deux cent cinquante cas réels. Avec quelques statistiques en prime.

RSA Conference 2009, San Francisco. Rien ne vaut l'enseignement par l'exemple ! C'est probablement ce que ce sont dits les chercheurs de l'université américaine de Carnegie Mellon / CERT en venant présenter quelques cas de fraude interne tirés de leur recherche dans le domaine.

L'objectif des chercheurs est double : d'abord, bien entendu, collecter des données afin d'en tirer des statistiques. C'est ainsi que l'on apprend que la majorité des cas de fraude interne (38%) a lieu dans le seceur IT. Les secteurs du gouvernement (22%) et de la finance (21%) consituent sans trop de surprise les deux autres domaines les plus frappés.

Autre chiffre intéressant, l'étude du CERT dévoile que 68% des personnes ayant dérobé des informations confidentielles à leur société l'ont fait les trois semaines précédant leur départ lorsque celui-ci était prévu (de quoi être, peut-être, plus vigilant durant cette période, ou au moins avoir une idée jusqu'où remonter dans les logs en cas de problème !).

Mais le coeur de la recherche menée à Carnegie Mellon consiste à établir un "modèle" de la fraude interne (les scientifiques aiment les modèles !) afin de tenter de la prévenir. Si cet aspect là des recherches n'est pas terminé, CERT est venu livrer quelques exemples de fraudes réelles issus de leur base de 250 cas avérés auxquels ils ont pu avoir accès.

Petit florilège des méthodes utilisées par les fraudeurs :

- Le tour de passe-passe : un employé revenu de nuit sur son lieu de travail a pris le temps d'échanger les plaques nominatives entre son bureau et celui d'un collègue, puis est allé demander au veilleur de nuit de lui ouvrir "son" bureau car il en avait oublié les clés. Il a ainsi pu copier le contenu du poste de travail du collègue.
- Le contournement : L'entreprise avait des processus de dé-provisonnement efficaces et l'employé licencié le vendredi après-midi perdait immédiatement accès à tous ses comptes... logiques. Mais son accès physique n'ayant pas pu être révoqué avant le lundi matin, il a pu revenir durant le week-end et déclencher l'arrêt d'urgence de l'électricité dans la salle des serveurs.
- Les identités multiples : Avant d'être licencié cet administrateur réseau a pris soin de créer des comptes VPN pour le CEO et le CFO, qui manifestement n'en n'avaient aucune utilité. Ainsi, même privé de ses accès par un processus de dé-provisionnement efficace, l'employé a pu conserver un accès privilégié au Système d'Information pendant plusieurs semaines, et cela bien entendu sans éveiller de soupçons.
- Le commentaire de trop : Le développeur travaillant pour une société de lotterie américaine avait bien entendu accès aux codes sources. Il a ainsi pu commenter une ligne : celle qui permettait d'alerter l'équipe sécurité lorsqu'une interface spécifique, rarement utilisée, était appelée. Il se trouve que cette interface permettait de vérifier manuellement la validité d'un billet gagnant en entrant son numéro de série...
- Le robinet reste ouvert : Chaque lundi en arrivant à son bureau cet administrateur réseau ouvrait une connexion SSH vers une machine installée à son domicile. Et lorsqu'il a été licencié pour faute grave avec interdiction de revenir à son poste de travail (et tous ses accès révoqués dans la foulée), il disposait toujours en arrivant chez lui d'un accès complet et privilégié au réseau. Ce qui lui a permis de détruire plusieurs systèmes auxquelles il avait accès.

Le CERT reconnaît bien volontier ne donner aucun conseil pour l'instant et se contenter d'amasser les données. Mais ces exemples illustrent dores et déjà l'importance des contrôles adéquats à mettre en oeuvre au sein de l'entreprise (contrôle du changement, procédures de revue par les pairs, etc...) au delà du seul deprovisionning qui se révèle faillible face à un attaquant déterminé.

- Le site de la recherche anti-fraude du CERT.

*Post-scriptum :*

http://www.securityvibes.com/fraude...