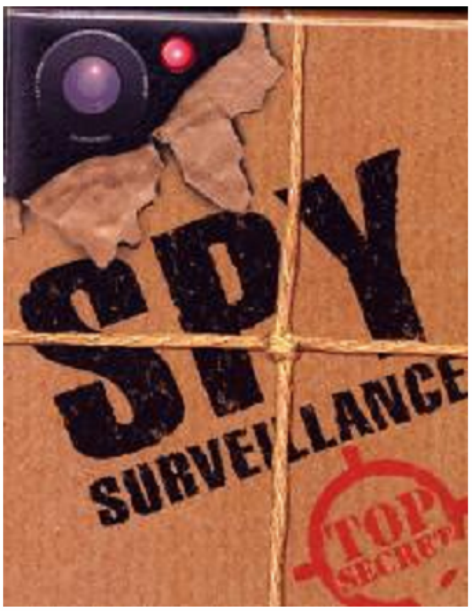
SAMEDI, MARS 18, 2006

ESPIONNAGE: LA MENACE VIENT DE L'INTÉRIEUR

Second volet de notre série sur l'espionnage industriel et l'informatique, avec ici plusieurs conseils pour les entreprises.

Jérôme Plantevin

En matière de vol d'informations stratégiques et de piratage informatique, la menace vient très souvent de l'intérieur de l'entreprise, et non simplement de quelque lointain cyberpirate."Mais il y a encore peu d'entreprises sensiblisées aux risques d'une gestion laxiste des employés concernant la sécurité", souligne Michel Kabay, directeur de la maîtrise en sécurité informatique à l'Université Norwich, au Vermont.



Pendant l'événement La Boule de Cristal du CRIM, tenu en février, M. Kabay a sensibilisé les gestionnaires québécois à leur rôle dans la lutte contre l'espionnage industriel. "Les trois quarts des cas connus d'espionnage et de dommages informatiques en entreprise, au cours des 25 dernières années, ont pour origine les employés", souligne M. Kabay."C'est pourquoi il est important de faire les gestes qui limitent les risques internes de fuite d'informations, tant lors de l'embauche d'un employé, d'un stagiaire ou d'un consultant, que durant son travail et son congédiement ou départ", ajoute-t-il.

Lors de l'embauche

Avant d'embaucher un employé, un stagiaire ou un consultant, le gestionnaire devrait :

> Porter attention à l'historique de travail de la personne et surtout vérifier ses antécédents avec soin.

> Lui faire signer des contrats légaux. Lui imposer l'adhésion aux politiques de l'entreprise ou encore lui faire signer des clauses de protection de la propriété intellectuelle avec des accords de non-divulgation des secrets commerciaux et d'informations.

Durant la durée de l'emploi

Selon M. Kabay, la moitié des cas d'espionnage, de détérioration et de pertes de données informatiques stratégiques viennent de l'incompétence et du manque d'attention des employés, ou encore d'un manque d'encadrement, de sensibilisation et de formation à la problématique de la sécurité."Quelque 10 % de ces cas seraient dus à des employés mécontents, 10 % à des employés malhonnêtes et le reste [environ 30 %] à des facteurs externes", dit-il.

Il est donc important :
> D'identifier les circonstances pouvant favoriser les actes d'espionnage. "Pensez comme un criminel et cherchez à contourner les règles", conseille M. Kabay. Une fois cet exercice effectué, l'entrepreneur devra préparer des contre-mesures, comme la mise en place de procédures de vérification systématique, ou d'un plan pour contrer adéquatement les tentatives de corruption qui peuvent viser des employés.
> De gérer très strictement l'accès au réseau informatique et aux ordinateurs. Chaque utilisateur doit avoir uniquement accès aux données dont il a besoin."Je conseille de vérifier l'historique de crédit de toutes les personnes qui ont directement ou indirectement accès aux ressources et aux mots de passe donnant des privilèges d'administrateurs de réseau", dit Jacques Viau, directeur de la sécurité pour le CRIM et l'Institut de sécurité de l'information du Québe.
> d'empêcher les employés de s'échanger leurs mots de passe et leurs cartes d'accès. "Il n'y a rien de pire qu'un directeur qui confie ses mots de passe à sa secrétaire, ajoute M. Viau. L'entreprise a vérifié si le directeur n'a pas de faiblesses qu'un espion pourrait exploiter, mais ne l'a pas fait dans le cas de la secrétaire."
> D'installer des logiciels de suivi des actions des utilisateurs. Cela permet de voir si un employé est parvenu à accéder à un serveur stratégique, alors qu'il n'avait aucun accès privilégié.
> De surveiller les changements de comportement chez les employés. Un employé peu fortuné qui affiche du jour au lendemain des signes ostentatoires de richesse ou encore un directeur bougon qui commence brusquement à faire de grands sourires sont autant de signes révélant qu'il y a anguille sous roche.
> De ne pas accorder à la même personne l'autorisation et l'exécution d'une fonction stratégique, comme la création puis l'installation d'un nouveau programme informatique. La séparation des fonctions oblige la collaboration de plusieurs personnes, ce qui complique la vie d'un espion.
> D'informer les employés des comportements à risque en leur donnant des exemples d'espionnage industriel, comme ceux que nous avons présentés dans notre dernier numéro.
> D'interdire l'installation de logiciels, sans autorisation.
> D'interdire les tests de sécurité informatique qui n'ont pas été préalablement autorisés.
> D'aviser les employés de ne pas coopérer à de présumées nouvelles procédures de sécurité, sans s'assurer qu'elles ont vraiment été demandées par la haute direction.
> De gérer intelligemment l'utilisation des ordinateurs sans fil et des assistants personnels des employés (comme un BlackBerry) qui détiennent ou ont accès à des données stratégiques. Cette mesure s'applique tant au stagiaire qui utilise une clé USB pour enregistrer des données concernant son rapport de stage, qu'au cadre supérieur et au consultant qui emportent des dossiers stratégiques avec eux."Trop d'entreprises se contentent de demander à leur consultant externe d'installer seulement un logiciel antivirus sur leurs portables", observe Robert Masse, président de GoSecure. Crypter les données présentes sur les disques durs de ces appareils sans fil peut être une solution.

Lors du départ

Les entrepreneurs devraient se donner une procédure de suppression des privilèges des employés congédiés, des stagiaires et des consultants qui quittent leur entreprise.

Cette procédure devrait garantir que l'entreprise :
> Récupère les cartes d'accès.
> Reprend les ordinateurs et autres clés USB lui appartenant.
> Vérifie que les appareils sans fil personnels utilisés dans le cadre du travail ne contiennent plus de données ni de documents d'entreprises tels que des formulaires ou des listes de clients.
> S'assure que les nom et mot de passe de l'employé ne servent plus à accéder au réseau, le jour même du départ.
> Ferme le compte de courriel de l'employé qui s'en va.

Source: Les Affaires, jeudi 15 mars 2006, Section Technologies

Publié par Jérôme Plantevin à 8:37 AM