



Article de Mathieu Grignon
Directeur des services de sécurité
ESI Technologies de l'Information inc.

Ce qu'il faut savoir sur l'enquête informatique

L'enquête informatique est une discipline relativement nouvelle, qui connaît une ascension rapide. Traditionnellement, elle a été confiée aux corps policiers. Ceux-ci, toutefois, se retrouvent aujourd'hui débordés, en raison de la recrudescence des crimes de nature informatique, engendrée par l'utilisation presque généralisée de l'ordinateur dans le travail et la vie de tous les jours. Par conséquent, les plaignants font aussi appel à des enquêteurs privés, dont la réputation de discrétion constitue, dans certains cas, un motif supplémentaire d'avoir recours à leurs services.

Mais qu'est-ce que l'enquête informatique – que l'on appelle parfois *forensic*? Ni plus ni moins que l'enquête judiciaire traditionnelle appliquée au monde de l'informatique. Toute infraction réelle ou supposée comportant des éléments de preuve liés à l'informatique tombe dans cette catégorie. Les litiges ainsi traités sont nombreux : vols d'informations, délits d'initié, bris de contrat, disputes d'actionnaires, etc. Les intrusions faites par des pirates dans les systèmes d'une organisation peuvent aussi donner lieu à des enquêtes.

Les enquêteurs

Si les spécialistes de l'informatique foisonnent, tous ne peuvent pas mener une enquête. Après tout, un gardien de sécurité ne se convertit pas automatiquement en policier, et encore moins en enquêteur. Pareillement, un informaticien ne peut nécessairement être analyste de systèmes, par exemple, ni spécialiste de l'enquête.

En fait, il n'existe pas de profil type. Beaucoup d'enquêteurs informatiques sont des policiers ayant acquis cette spécialité, et beaucoup proviennent de divers autres milieux. Une organisation sera avisée de confier une enquête à des personnes d'expérience, ayant fait leurs preuves dans le domaine. L'enquêteur chevronné, en effet, saura comment s'y prendre pour présenter devant un tribunal une preuve recevable. Pour ce faire, il aura recours à la méthode dite des 3A – acquisition, authentification et analyse.

Acquisition

Afin de faciliter le travail des spécialistes, le plaignant ne doit pas tarder à mettre l'enquête en marche puisque la rapidité d'exécution accroît les probabilités que les preuves électroniques ne soient pas modifiées. Au préalable, il doit vérifier s'il doit obtenir une ordonnance de la cour, ce qui est normalement le cas lorsque la plainte regarde une autre entreprise que la sienne. À l'interne, l'ordonnance n'est habituellement pas requise. Le plaignant doit aussi considérer les clauses de certains contrats de travail interdisant l'accès aux informations personnelles d'un employé, notamment le courrier électronique.

Une fois ces modalités réglées, l'enquêteur peut entamer son travail. Souvent, il arrive sur les lieux du crime accompagné de huissiers. Il s'empresse de faire une copie binaire des disques durs qui seront utiles à l'enquête. Et pour s'assurer qu'il acquiert toutes les informations pertinentes, il ne devra oublier aucun bit : si les données dont il pense avoir besoin ne représentent que 10 Go, sur un disque de 100 Go, la copie devra tout de même inclure la totalité des 100 Go. Ainsi seulement pourra-t-il récupérer les données supprimées qui n'ont pas encore été remplacées dans les espaces qui leur étaient réservés avant la suppression.

Et puisque la règle d'or consiste à ne pas altérer les données, on utilise des logiciels spécialisés, dotés de mécanismes de protection en écriture. Les enquêteurs feront une première copie, sur laquelle ils pourront chercher les preuves sans crainte de modifier les données originales. Ils en feront aussi une deuxième, dans l'éventualité où la première ne serait plus utilisable. Enfin, ils prendront soin de faire les copies à l'aide de logiciels différents, au cas où il serait déterminé plus tard, qu'un bogue entrave le bon fonctionnement de l'un d'eux.

Parce que la mémoire est une faculté qui oublie, tous les détails doivent être notés au bénéfice du tribunal, qui pourrait ne siéger que bien plus tard : versions des logiciels utilisés, état des ordinateurs, volume des données, programmes installés, etc. Pour la poursuite de l'enquête, il est capital que, du premier coup, les choses soient faites de façon impeccable. Il s'avérera donc très difficile, voire impossible, de réparer les erreurs commises à ce stade.

Authentification

L'objectif de l'authentification est de prouver au juge que les données qui lui sont présentées sont exactement les mêmes qu'au moment où elles ont été recueillies. À l'aide de ce qu'on appelle un algorithme de *hachage*, les enquêteurs convertissent les données en une chaîne de caractères, à laquelle on attribue une empreinte. Le moindre changement apporté aux données, ne serait-ce qu'un bit sur plusieurs milliards, provoque la modification de l'empreinte.

Analyse

L'analyse des données consiste donc à examiner les traces laissées par l'exécution de tâches informatiques. On retrouve des traces dans les listes de contrôle de divers éléments de l'infrastructure technologique : serveurs, applications, pare-feu, etc. Pour remonter les faits, l'enquêteur ne doit négliger aucune piste. Ainsi, les courriels et les séances de clavardage pourraient être minutieusement fouillés, de façon à trouver des indices quant aux intentions des suspects. On prendra aussi soin d'examiner les serveurs sur lesquels sont demeurées des traces des activités d'utilisateurs passés, même lorsque les données ont été supprimées de leur poste de travail.

À cette étape, encore, le recours à un spécialiste revêt une importance particulière. Même si, en théorie, n'importe quel informaticien est en mesure de procéder à l'analyse des données, il n'est pas dit combien de temps devra mettre un néophyte pour obtenir les résultats escomptés, ni le volume d'efforts qu'il devra déployer afin d'y arriver. Ce type de travail revient souvent à chercher une aiguille dans une botte de foin car pour trouver des informations précises dans des masses de données, emmagasinées dans une variété de supports, il convient de bien connaître les techniques de recherche et les outils spécialement conçus à cette fin.

Conservation des données

La nécessité d'analyser les données soulève deux questions clés : quelle quantité d'informations doit-on conserver, et durant combien de temps? Car on ne peut perdre de vue les coûts importants se rattachant au stockage à long terme de grands volumes de données. Aujourd'hui, une partie de la réponse se trouve dans l'obligation faite aux entreprises par des réglementations comme la loi Sarbanes-Oxley et, au Canada, la loi 198, de conserver certaines informations.

Pour le reste, on doit s'en remettre au principe de l'équilibre entre le coût à défrayer et le risque à encourir. Un précepte lié à la gestion du risque veut que s'il en coûte, par exemple, 20 000 \$ pour protéger de l'information dont la valeur n'est que de 10 000 \$, le jeu n'en vaut pas la chandelle. Autre facteur qui pourrait peser lourd dans la décision : les traces ne servent en rien à prévenir, mais uniquement à guérir!

Intrusion dans les systèmes

Lorsque l'enquête porte sur une intrusion dans les systèmes d'une organisation, la première initiative des enquêteurs sera de déterminer par où elle a eu lieu, de façon à fermer la porte à toute autre attaque. Ils vérifieront ensuite jusqu'où les pirates ont réussi à pénétrer, afin d'évaluer l'étendue des dégâts. Enfin, les organisations animées d'une forte dose de détermination et qui croient pouvoir compter sur le concours de Dame Chance confieront aux enquêteurs la tâche de trouver les coupables – ce qui peut s'avérer fort complexe, particulièrement si l'attaque a été lancée de l'étranger.

De nombreuses victimes d'intrusion hésitent à faire appel à des enquêteurs, de peur que l'incident ne s'ébruite et que leur réputation n'en souffre. Mais il n'y a pourtant pas de honte à cela puisque le système de sécurité parfait n'existe pas. Même les organisations les mieux protégées sont vulnérables, surtout lorsqu'elles possèdent des informations convoitées. Ainsi, personne ne se surprendra si un commerce de bijoux, pourtant protégé par une sécurité haut de gamme, est cambriolé sans que ne le soit la maison voisine, où il n'y a même pas de système d'alarme.

Dépôt du rapport d'enquête

Une fois qu'il a en main le rapport d'enquête, le plaignant doit décider de la suite des choses. Selon les conclusions qui lui sont présentées, il peut intenter des poursuites, chercher à obtenir une entente hors cour, congédier du personnel, accroître les mesures de sécurité entourant ses systèmes, abandonner le dossier, etc. En cas de poursuite, les enquêteurs seront vraisemblablement appelés à la barre des témoins.