LE COIN DE LA SÉCURITÉ INFORMATIQUE

SÉCURIT

La protection des renseignements personnels... Est-ce *nécessaire?*

Les spécialistes mentionnent souvent la ***confidentialité,*** l'***intégrité*** et la ***disponibilité*** comme étant les trois grandes préoccupations autour desquelles doit s'articuler toute étude sérieuse sur la sécurité informatique. Des trois, la notion de ***confidentialité*** est celle le plus fréquemment associée à la sécurité, tandis que l'***intégrité*** et la ***disponibilité*** sont considérées par le profane comme des aspects « techniques », liés exclusivement aux systèmes. En fait, ce sont trois aspects indispensables et d'égale importance.

En réalité, la ***confidentialité*** a deux aspects. Vous êtes sans doute au courant qu'il faut protéger l'information stockée dans les systèmes informatiques parce qu'elle est de nature délicate ou qu'elle a trait à l'intérêt national, et vous êtes sûrement conscient que si elle était divulguée aux « mauvaises » personnes, l'intérêt national en souffrirait.

Cependant, le lien entre la ***confidentialité*** et le « droit à la vie privée » est moins évident. Les entreprises de partout dans le monde adoptent à l'égard de leurs installations informatiques des attitudes fort variées, qui se situent entre deux stéréotypes diamétralement opposés. Certaines maintiennent que, parce que les systèmes informatiques leur appartiennent, toute l'information traitée doit se rattacher directement aux activités de l'entreprise. À l'autre extrême, il y a des sociétés qui n'exercent aucun contrôle (et qui ne souhaitent peut-être pas le faire).

Mettons que, dans la plupart des cas, les entreprises adoptent une attitude entre ces deux extrêmes. Toute personne raisonnable conviendra qu'une entreprise est en droit de s'attendre à ce que le matériel dont se sert son personnel soit utilisé pour les besoins de l'entreprise, mais que, à l'occasion, cette dernière se montrera assez souple et « humaine » pour accepter qu'il serve à des fins personnelles, sans pour autant nuire à ses activités, ni susciter de conflit d'intérêt.

Et quel est le point de vue du ministère des Affaires étrangères et du Commerce international à ce sujet? Il va de soi que pour le traitement, le stockage et la transmission des données du Ministère, les employés doivent se servir des systèmes approuvés, être conscients de leurs limites au chapitre de la protection des renseignements et les respecter. Ainsi, vous ne devez pas utiliser le SIGNET-D (version « désignée » du SIGNET et le matériel à votre poste de travail, au lieu de la version protégée du SIGNET, c'est-à-dire le SIGNET-C) pour traiter, stocker et transmettre des données ayant une cote supérieure à PROTÉGÉ-A. Le système n'est tout simplement pas doté des dispositifs requis pour assurer le degré de confidentialité nécessaire. Pour savoir quel système utiliser, demandez-vous si vous seriez à l'aise de voir l'information à la une du journal de demain. Si la réponse à cette question est « non », ne traitez pas l'information sur le SIGNET-D. Ce système a été conçu pour le traitement et la protection des données ayant la cote PROTÉGÉ-A ou moins, rien de plus, ce qu'il fait avec efficacité.

Et les renseignements « personnels »? Combien de personnes ***devraient*** pouvoir lire votre courrier électronique? Combien de personnes ***peuvent*** le faire? À quel degré de confidentialité pouvez-vous vous attendre si vous traitez des données sur le SIGNET-D, si vous imprimez sur le SIGNET-D ou si vous stockez l'information sur une disquette : votre unité C:, votre unité I: ou votre unité H:? Partez du principe qu'il n'y a rien de confidentiel sur le SIGNET-D. Si vous traitez des renseignements que vous ne souhaitez pas divulguer, vous devriez probablement les sauvegarder sur une disquette, que vous pourrez alors ranger dans un endroit sûr.

L'utilisateur du SIGNET-D qui veut prendre une décision éclairée quant au genre d'information à traiter sur le système doit savoir ce qui suit :

1. Les administrateurs de systèmes sont omnipotents, ou presque, et qu'ils peuvent faire, voir et lire ce que bon leur semble. Cela ne signifie pas cependant qu'ils vont effectivement **tout lire**, mais tout simplement qu'ils le **peuvent**. En réalité, comme nous tous, ils ont leur boulot à faire et sont bien trop occupés pour fureter et fourrer leur nez dans les affaires des autres.

2. Un grand nombre des données circulant sur le SIGNET-D (surtout le courrier électronique des missions) sont transmises par satellite sans être chiffrées. N'importe qui possédant une antenne parabolique, ou soucoupe, peut recevoir les données transmises par satellite et en prendre connaissance à sa guise sans être importuné.

3. Le système ne traite pas différemment le courrier électronique du seul fait qu'il porte la mention PROTÉGÉ. Il faut considérer que cette directive s'adresse au destinataire, et non au système.

4. Partez du principe que les données stockées sur l'unité C: de votre ordinateur ne sont pas protégées. Trop de gens nous ont raconté qu'ils avaient fermé leur ordinateur le vendredi avant de partir, mais qu'à leur arrivée, le lundi matin, ils y avaient trouvé des jeux dont ils n'avaient jamais entendu parler. Quiconque se sert de votre ordinateur a accès aux fichiers qui s'y trouvent.

5. Partez du principe que vos unités I: et H: ne sont pas protégées. Tout le personnel du Secteur a accès à votre unité I:, et un grand nombre d'administrateurs de systèmes, à votre unité H.

6. Ne supposez jamais que vous ne risquez rien parce que vous n'allez qu'imprimer. Le fait est que votre projet d'impression part de votre ordinateur et est acheminé au serveur du réseau, où il attend que l'imprimante choisie soit prête à le recevoir. Votre texte peut donc tomber sous les yeux de gens qui n'ont pas à le voir.

7. N'allez pas vous imaginer que « jamais personne ne lira ceci... », parce qu'en fait, bien des gens, pour des motifs qu'ils sont les seuls à connaître, parcourent les systèmes en quête de découvertes — à votre sujet en particulier ou tout simplement par oisiveté ou curiosité.

Vous auriez raison de conclure que l'information qui transite par ce système n'est pas à l'abri des regards indiscrets. À vrai dire, cela n'a jamais été l'un des objectifs visés pour ce système, qui fonctionne d'ailleurs très bien. L'important, c'est que les utilisateurs soient conscients des particularités du système et qu'ils agissent en conséquence. À l'heure où les ordinateurs se parlent davantage entre eux, de l'Internet et du village planétaire de McLuhan, on n'en sait jamais assez long sur la protection du caractère confidentiel de l'information — surtout l'information personnelle.