Internet à l'UQAM : la Toile est fragile

Dominique Forget

Photo : Michel Giroux

Hugo Dominguez, directeur de la sécurité informatique à l'UQAM.

Chaque mois en moyenne, 10 millions de courriels sont envoyés à des membres de la communauté de l'UQAM. De ce nombre, 8 millions sont des pourriels. Heureusement, le système de sécurité déployé par le Service de l'informatique et des télécommunications (SITel) arrive à intercepter la majorité d'entre eux avant qu'ils n'atteignent les boîtes de réception des usagers. Ceux qui démarrent leur ordinateur le matin ne se doutent aucunement des efforts qu'ont dû déployer les responsables de la sécurité pour assurer la fiabilité du réseau.

«Les pourriels qui ont des titres bien connus comme *Ben Laden Captured* ou *Enlarge your Penis* sont systématiquement interceptés», explique Hugo Dominguez, directeur de la sécurité informatique à l'UQAM. «Nous interceptons aussi les courriels qui contiennent un fichier attaché suspect. Par exemple, les fichiers qui ont une extension «.pif» ou «.cpl» sont souvent des virus. Si un message est identifié comme pourriel, on met l'expéditeur sur notre liste noire.»

Selon les périodes de l'année, la liste noire peut s'accroître quotidiennement de 1 000 expéditeurs… ou de 19 000! Cette liste n'est jamais parfaite. En effet, la nature et surtout la variété des activités des usagers de l'UQAM rendent le travail de l'équipe du SITel particulièrement compliqué. «Nous ne pouvons pas intercepter tous les courriels qui contiennent le mot «viagra», même si nous savons que le nom de ce médicament est généralement associé à des pourriels. Il risque d'y avoir des professeurs qui font des recherches sur le sujet, en sexologie ou en psychologie par exemple, qui n'arriveront pas à recevoir des courriers légitimes. La ligne entre les bons et les mauvais courriels n'est pas toujours claire. Nous travaillons toujours dans des zones grises. On tente de fixer les balises au meilleur de notre jugement, mais il arrive que des pourriels se faufilent dans le réseau ou, inversement, que des courriels soient inutilement interceptés. Les expéditeurs sont toutefois avisés de l'opération et de la procédure à suivre pour être éliminés de la liste noire.»

Attaques ciblées ?

Une fois qu'un virus a réussi à infecter un ordinateur, il tente généralement de se propager. Certains d'entre eux sont programmés pour faire plus de 65 000 tentatives de connexions à la seconde, ce qui engorge les bandes passantes. «C'est généralement le moment où les usagers se plaignent de la lenteur de leur machine, note M. Dominguez. Il suffit d'une personne qui ne fait pas attention et qui laisse un virus s'installer sur son ordinateur pour que plusieurs usagers du réseau soient pénalisés.»

Selon Omar Cherkaoui, professeur au Département d'informatique de l'UQAM et Directeur du laboratoire de téléinformatique, les pirates visent de moins en moins les machines et de plus en plus les réseaux comme tels. «Les nouveaux virus s'attaquent par exemple aux routeurs et aux commutateurs : deux équipements essentiels au fonctionnement du réseau. Les pirates y accèdent par toutes sortes de canaux, pas seulement les courriels. Les attaques sont de plus en plus subtiles.»

Entre le mois d'août 2003 et le mois de mai 2004, l'UQAM a fait l'objet de sept attaques majeures de virus qui ont entraîné des coûts substantiels pour la communauté. L'origine de ces attaques n'est pas toujours connue ou du moins divulguée, mais pour Omar Cherkaoui, il est clair que certaines d'entre elles visaient directement l'UQAM. «Le réseau Internet a été bâti avec un code informatique qui est connu de tous, dit-il. N'importe quelle personne futée qui connaît bien l'informatique peut lancer des attaques.»

Politique de sécurité

L'UQAM travaille actuellement à se doter d'une Politique de sécurité informatique. Quatre professeurs et cinq représentants des services administratifs se sont réunis à de nombreuses reprises avec le Vice-recteur aux services académiques et au développement technologique, Claude-Yves Charron, pour jeter les bases du document qui fait actuellement l'objet d'une consultation. «Nous voulons, d'une certaine manière, baliser le travail que font les usagers sur le réseau. Il n'est pas question de restreindre leur liberté, mais nous souhaitons les sensibiliser à l'impact de leurs comportements, à l'importance de faire des mises à jour de leur antivirus par exemple. Leur négligence coûte très cher à l'UQAM. Pour nettoyer un seul ordinateur, un employé du SITel met environ 3 heures. Si 300 ordinateurs sont infectés par un virus, ça représente 900 heures, la moitié d'une année complète de travail pour un employé.»

La sécurité du réseau est devenue encore plus critique depuis que l'Université a initié la conversion du système téléphonique traditionnel vers la téléphonie IP. Le système téléphonique antérieur était vétuste et l'UQAM a choisi d'adopter la technologie la plus avancée qui soit. Ainsi, les conversations téléphoniques ne transigeront plus sur de bonnes vielles lignes téléphoniques, mais sur le réseau informatique interne. Advenant une panne, les communications à partir de l'ordinateur et du téléphone deviendraient non disponibles. Le SITel travaille toutefois à configurer le réseau de façon à éviter ce scénario catastrophe.

Pour Omar Cherkaoui, l'idée de mettre en place une politique est un bon premier pas, mais il est loin d'être suffisant. «Les pirates ne vont pas arrêter de lancer des attaques du jour au lendemain parce que l'UQAM a adopté une politique, souligne-t-il. Les usagers peuvent télécharger les antivirus, ça aidera certainement, mais les pirates trouveront autre chose. La sécurité informatique, c'est comme un jeu d'échec. Il faut être plus futé que les pirates. Il faut former des informaticiens hautement qualifiés qui seront en mesure d'anticiper les coups et de préparer notre réseau en conséquence. Les anciens pirates font souvent les meilleurs agents de sécurité. Mais on aura beau faire n'importe quoi, il y aura toujours un risque. La seule solution pour protéger nos données, prévient le professeur en riant, c'est de se débrancher!» ●