Haro sur le cybervandalisme

Les pirates constituent une population hétérogène : leurs profils et leurs motivations sont divers et ils disposent de moyens financiers variables. Les protections à déployer à leur encontre doivent combiner prévention et détection des intrusions.

ETIENNE LEVESQUE
Product manager

STÉPHANE WOILLEZ
Security architect
Tivoli

Qu'est-ce que le cybervandalisme ?

Ce concept recouvre principalement deux types d'attaques lancées à l'encontre d'un site : les virus et les intrusions. Lorsque nous sommes sollicités pour sécuriser un site, ce sont ces aspects qui sont le plus souvent exprimés. Même si on observe un intérêt grandissant pour un modèle de sécurité assurant la confidentialité des données au sens que lui donne la CNIL ou la sécurisation des transactions de commerce électronique.

Peut-on dresser une typologie des cybervandales ?

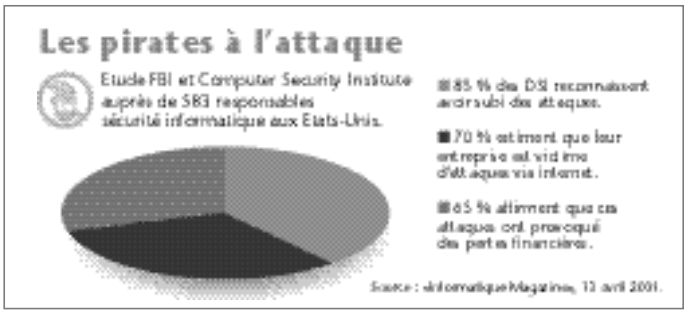
Celle-ci recouvre une grande diversité de *hackers*, dont les moyens financiers vont croissant : les indépendants, les organisations criminelles, mais aussi des entreprises voire des États… Leurs motivations sont multiples : la célébrité pour certains, la vengeance, par exemple d'un salarié évincé, la destruction de données ou de documents, l'espionnage ou le vol de ces données. Ils peuvent aussi s'introduire sur un site qui leur servira de couverture pour en attaquer un autre. La manœuvre, outre l'intrusion, pose un problème juridique car il reste à la charge de l'entreprise utilisée comme «site de rebond» de prouver qu'elle n'est pas responsable. Enfin certains sites ont subi ces dernières années des «denis de services» : dans ce cas il ne s'agit pas de vol de données mais de submerger d'appels le site jusqu'à le bloquer. L'impact de ces actes est très violent pour une entreprise. Il ternit durablement son image et peut faire douter ses clients de sa capacité à sécuriser son site.

Quelles sont les parades efficaces ?

Deux méthodes existent : la prévention et la détection. Longtemps, les entreprises se sont contentées du volet prévention, mais l'expérience montre que comme pour une maison, les deux types d'alarmes doivent être activés.

La prévention, avec la mise en place des *firewalls* et de logiciels anti-virus et la détection des attaques. Les sites aux Etats-Unis n'hésitent d'ailleurs pas à mentionner les systèmes de sécurité qu'ils utilisent pour rassurer leurs clients. Les entreprises françaises s'y refusent encore car elles ne veulent pas renseigner les pirates, mais, en pratique, ceux-ci ne mettent pas longtemps à identifier les techniques employées. IBM a par ailleurs des équipes de *ethical hackers* : ils aident les entreprises à tester la robustesse des sites, à détecter les failles et vérifier l'efficacité des procédures d'alertes.

La détection quant à elle, peut prendre la forme de deux approches : la plus répandue se fonde sur la connaissance et vise à repérer tout élément suspect. La seconde, fondée sur une analyse comportementale, consiste au contraire à considérer comme suspect tout ce qui n'est pas normal. En pratique, la combinaison des deux techniques aboutit à une meilleure efficacité.



Plus globalement, il faut également faire en sorte que le chargé de la sécurité dans l'entreprise ait le temps et les moyens de se consacrer à ces questions. Souvent il passe 50 % de son temps à créer ou gérer les mots de passe des utilisateurs du système d'information, c'est-à-dire à des tâches sans réelle expertise, ni beaucoup de valeur ajoutée. Il existe aujourd'hui des solutions qui industrialisent l'administration des utilisateurs. ●

Propos recueillis par E. C.