Quelques leçons sur la sécurité après les piratages de Twitter

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 mars 2010

https://www.bortzmeyer.org/twitter-lecons-securite.html

Le piratage de plusieurs comptes Twitter, dont celui d'administrateurs du site Web, puis ceux de clients célèbres comme Barack Obama, par un nommé Hacker-Croll <http://www.zataz.com/news/20044/hacker-croll--hackercroll--hacker-croll.html> a suscité beaucoup d'intérêt médiatique... bien à tort.

Comme souvent avec les piratages spectaculaires sur l'Internet, on a fait une montagne d'une taupinière. Aucune technique nouvelle n'a été utilisée, Hacker-Croll a surtout utilisé (avec compétence et ténacité) des méthodes non-informatiques classiques et très connues : il existe des tas de comptes sur l'Internet qui ne sont protégées que par des barrières très faibles (comme une question « Où ai-je rencontré ma femme ? », s'agissant d'une personnalité publique dont la biographie est bien connue...). Que quelqu'un aie réussi à passer outre ces barrières n'est pas une information. Ferait-on les gros titres avec une information comme quoi quelqu'un a réussi à voler une voiture ? Ou à cambrioler un appartement ?

Mais, va t-on me dire, c'étaient les compte de personnes importantes. Et alors, qui peut croire que ces comptes servaient à autre chose qu'à faire envoyer des communiqués par un employé du service de presse de la Maison Blanche ? Que croient les journalistes qui ont frissoné en annonçant que le compte d'Obama était piraté ? Qu'on peut lancer les ICBM depuis Twitter ? Ce compte ne servait pas à grand'chose et son piratage n'a guère d'importance. C'était exactement la même chose avec des comptes sans intérêt comme le compte Hotmail d'un député godillot <http://www.numerama.com/magazine/15268-pirate-le-depute-philippe-goujon-porte-plainte-mais-prend-ses-electeurs-pour-des-im
html>. Que pouvait-il y avoir dans la boîte aux lettres d'un député UMP de base ? Certainement pas des secrets d'État.

J'ai même pu lire des indignations que la sécurité de Twitter soit si mauvaise (ce n'est pas, et de loin, leur premier problème de sécurité). Ces indignations sont doublement ridicules. D'abord, elles oublient une règle de base de la sécurité (pas seulement informatique) : il n'y a pas de sécurité parfaite, il n'y a que des compromis. Renforcer la sécurité coûte (du temps, de l'argent, des ennuis) et il est parfaitement logique et légitime de limiter les coûts en ne cherchant pas à sécuriser à tout prix une ressource dont

l'importance est faible. Sécuriser son compte Twitter ou Hotmail, c'est une occupation pour le lycéen boutonneux qui se prend pour un hacker, pas une activité économiquement rationnelle.

Et cela nous mène à la seconde raison de ne pas être indigné ou même surpris par les failles de Twitter : **ce n'est pas un service critique** ! C'est un jouet pour faire mumuse <https://www.bortzmeyer.org/debut-twitter.html>, pas un élément essentiel qu'il faudrait protéger à tout prix. Twitter a aujourd'hui des revenus pratiquement égaux à zéro (je parle bien des revenus, pas des bénéfices). Les cervelles d'oiseau qui réclament qu'on sécurise le service de microblogging sont-ils prêts à payer pour cela ?