Le rejet des règles de sécurité peut être raisonnable

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 décembre 2009

http://www.bortzmeyer.org/rational-security.html

Si les utilisateurs s'obstinent à violer les règles de sécurité que les spécialistes de sécurité leur imposent, est-ce parce qu'ils sont bêtes et obstinés ? Ou bien parce qu'il font un calcul plus raisonnable qu'on ne pourrait le penser ? Un économiste tente de répondre à la question.

Cormac Herley, dans son article « "*So Long, And No Thanks for the Externalities : The Rational Rejection of Security Advice by Users*" <http://research.microsoft.com/en-us/um/people/cormac/papers/2009/solongandnothanks.pdf> » étudie le comportement des utilisateurs, lors de questions de sécurité informatique, à la lumière de calculs économiques rationnels. Excellent article, très provoquant. Sa thèse est que l'insistance des responsables de sécurité informatique, ou des informaticiens, à exiger des utilisateurs qu'ils appliquent des règles de sécurité contraignantes est non seulement sans espoir (ce que tout informaticien a déjà pu constater) mais également inappropriée. Les mesures de sécurité coûtent cher et il n'y a quasiment jamais d'analyse coût/bénéfice de celles-ci. On demande aux utilisateurs de passer du temps, donc de l'argent, pour résoudre des problèmes qui ne se posent finalement que rarement.

Un des meilleurs exemples de Cormac Herley concerne les certificats X.509. Lorsqu'une alerte de sécurité survient, il s'agit dans la quasi-totalité des cas d'une fausse alerte (certificat signé par une CA qui n'est pas dans le magasin, magasin qui est rempli assez arbitrairement, ou bien certificat expiré). Les vraies attaques sont très rares. Une analyse coût/bénéfice rationnelle comparerait le produit de cette probabilité d'attaque par le coût d'une attaque réussie, avec le coût des mesures de sécurité (ne pas pouvoir accomplir la tâche souhaitée). Et cette analyse dirait probablement que l'utilisateur qui s'obstine à passer outre l'avertissement et le parcours du combattant qu'impose Firefox 3 pour ignorer l'alarme, cet utilisateur est raisonnable.

Même chose avec l'analyse des URL dans le navigateur pour tenter de détecter une tentative de hameçonnage. Même si cette analyse ne prend que dix secondes par utilisateur, multipliée par le nombre d'utilisateurs et leur salaire horaire, cette vérification coûterait plus cher que le hameçonnage (l'article comprend un calcul détaillé, dans le cas des États-Unis). C'est bien la raison pour laquelle toutes les

études sur le hameçonnage montrent qu'il n'y a pas d'utilisation de noms de domaines « confondables » (contrairement à ce qu'on lit souvent pour s'opposer aux noms de domaine en Unicode <http://www.bortzmeyer.org/idn-et-phishing.html>).

Je ne dis pas que je suis d'accord avec l'auteur en tout. Il oublie de prendre en compte les effets rebonds (certaines attaques sont très rares mais, si on baisse la garde en pensant que les précautions coûtent trop cher, le nombre d'attaques va augmenter). Et les utilisateurs ne sont pas forcément rationnels car ils sous-estiment (souvent) ou sur-estiment (plus rarement) certains risques techniques. Mais Cormac Herley a le mérite de poser enfin le problème : dans certains cas (mots de passe par exemple), on n'a presque pas de données sur les attaques réussies par suite d'une trop faible sécurité. Alors, faut-il continuer à prôner aveuglément des mesures de sécurité, sans aucune mesure de leur rentabilité ?