Les conséquences inatendues des changements trop fréquents de mots de passe

Les conséquences inatendues des changements trop fréquents de mots de passe

Il est préférable d'opter pour des mots de passe robustes, plutôt que d'imposer des changements fréquents, réaffirme la responsable des technologies de la FTC.

Fraîchement nommée chef des technologies de la Federal Trade Commission (FTC), Lorrie Cranor (également professeur à l'université Carnegie Mellon), avait été surprise par un tweet officiel mis en ligne en janvier. Le régulateur américain du commerce préconisait alors un changement fréquent de mots de passe. La spécialiste s'y est opposée. Depuis, elle fait évoluer la politique interne sur le sujet.

« Je suis allée voir les personnes en charge des médias sociaux et leur ai demandé pourquoi [la FTC dit à tout le monde de changer de mots de passe] », a commenté Cranor lors de la conférence *Passwords* de BSidesLV 2016, dont *Ars Technica* s'est fait l'écho. *« Elles m'ont répondu ceci : 'C'est probablement un bon conseil, car à la FTC nous changeons nos mots de passe tous les 60 jours' »*.

Lorrie Cranor s'est alors entretenue avec le #DSI et le RSSI de la FTC. Elle a souligné, rapport d'experts à l'appui, que les changements fréquents n'améliorent pas la sécurité, mais encouragent au contraire l'utilisation de mots de passe plus susceptibles d'être découverts et détournés.

Un modèle, des mots de passe

Lorsque des utilisateurs doivent changer de mots de passe tous les 90 jours, par exemple, ils ont tendance à utiliser un même modèle. C'est ce qui ressort d'une étude publiée en 2010 par des chercheurs de l'université de Caroline du Nord (UNC) à Chapel Hill.

« Les utilisateurs prennent leurs anciens mots de passe, puis ils les changent légèrement [d'une lettre, d'un chiffre ou d'un symbole] pour obtenir un nouveau mot de passe », a expliqué Cranor. Or la capacité de ces mots de passe à résister aux attaques par force brute est faible. 17 % des mots de passe testés par les chercheurs de l'UNC auraient ainsi été découverts en moins de cinq tentatives.

Il est donc préférable, selon eux, d'utiliser des mots de passe forts, plutôt que d'en changer souvent. La double authentification est également recommandée, notamment pour les applications sensibles.

Article original de Ariane Beky

Réagissez à cet article

Original de l’article mis en page : Les changements fréquents de mots de passe nuisent à la sécurité