Techniques et astuces pour la robustesse de vos mots de passe

Techniques et astuces pour la robustesse de vos mots de passe

Les experts en cybersécurité ont tendance à être quelque peu cyniques envers les utilisateurs « lambda », particulièrement lorsqu'il s'agit du choix des mots de passe. Cependant, selon certains experts en sécurité informatique au sein du CyLab, l'Institut Security & Privacy de l'Université de Carnegie Mellon, les utilisateurs ordinaires ne semblent pas être aussi stupides qu'il n'y paraît. En effet les erreurs commises peuvent être classées en 4 catégories spécifiques. Le travail de sensibilisation nécessaire ne devrait pas être une tâche insurmontable.

La méthodologie de CyLab est la suivante : montrer aux gens des mots de passe par paires, et leur demander lesquels leur semblent les plus robustes. Ensuite, établir une corrélation entre leurs réponses et l'efficacité effective de ces derniers en utilisant *les méthodes les plus actuelles pour craquer les mots de passe*. Au final, sur 75 paires, les participants en ont correctement sélectionné 59. Il s'agit de 79%, soit en pratique un « B ».
Il est vrai que l'échantillon des 165 utilisateurs du CyLab est certainement un peu plus technique que d'autres utilisateurs : ils ont été recrutés en ligne via le système du Turc Mécanique d'Amazon. De plus, CyLab ne dit pas en substance que tous les utilisateurs atteindront ce score, mais seulement que certains peuvent y arriver. Enfin, pour conclure, ces scores ne sont pas alarmants.
Les personnes sondées par CyLab savaient que des mots de passe sont robustes lorsque :
• Les majuscules sont utilisées au milieu du mot, plutôt qu'au début.
• Des chiffres et des symboles sont situés au milieu du mot plutôt qu'à la fin.
• Des séquences de chiffres aléatoires sont insérées à la place d'autres plus évidentes, telles que l'année en cours par exemple.
• Des noms sont ajoutés, différents des traditionnels prénoms et noms.
• Des noms faisant parties de la vie privée ne sont pas utilisés, tels que les prénoms de vos enfants.
• Des mots faisant référence de manière évidente au site ou au compte que vous êtes en train de protéger ne sont pas utilisés.
Bien sûr, il en reste 21% qui n'ont pas réussi à faire la distinction. Cela laisse en effet de belles opportunités **aux cybercriminels pour craquer vos mots de passe**. Quelles ont donc été les plus grosses erreurs commises ? :
1. **Les participants ont ajouté des chiffres à leurs mots de passe, en plus des lettres, en pensant les renforcer**. Dommage ! Les hackers savent bien que les internautes très souvent rajoutent à la fin des chiffres, du coup « brooklynqy » est plus sécurisé que « brooklyn16 ».
2. **Les participants ont pensé que le fait de changer tout simplement des lettres en chiffres rendrait leurs mots de passe plus robuste.** Dommage ! Les craqueurs de mots de passe « exploitent de plus en plus la tendance des utilisateurs à faire des substitutions prévisibles », ainsi « punk4life » n'est pas plus sûr que « punkforlife ».
3. **Les participants ont surestimé la sécurité procurée par les séquences présentes au niveau de leur clavier.**Dommage ! Les hackers de nos jours recherchent très rapidement les séquences des claviers telles que « qwertyuiop », tout comme d'autres patterns classiques, et pas seulement à base de mots.
4. **Les participants ont mal appréhendé la popularité de certains mots ou de certaines phrases.** Selon le CyLab, par exemple, les utilisateurs ont pensé que « Leatsale88 » et « iloveyou88 » étaient équivalent d'un point de vue sécurité. Pas vraiment : les craqueurs de mots de passe ont besoin de plus d'un milliard de tentatives en plus pour en venir à bout de « ilovekale ». Il est plus sûr de choisir un mot isolé rare plutôt qu'une phrase intégrant « iloveyou » or « ilove ». Les mots de passe utilisant le mot « love » sont incroyablement répandus …ce qui est plutôt une bonne intention si vous n'êtes pas responsable de la cybersécurité d'un site.
Qu'est ce qui pourrait aider les utilisateurs pour éviter les mauvaises stratégies de choix des mots de passe ? Selon l'auteur de l'étude :
Une méthode qui semble être très efficace pour assister les utilisateurs dans l'évaluation de leurs mot de passe, vis-à-vis des pratiques courantes, est de leur fournir des feedbacks ciblés et explicites pendant la phase de création. Les calculateurs actuels de la force d'un mot de passe indiquent simplement aux utilisateurs si un mot de passe est faible ou fort, mais ne mentionne pas les raisons.
Les futurs travaux dans ce domaine pourraient s'inspirer d'une récente étude qui montrait la possibilité pour les utilisateurs de finir automatiquement le mot de passe partiel qu'ils viennent de taper … et pourrait également se baser sur une autre étude utilisant des arguments de motivation ou encore la pression de collègues pour inciter les utilisateurs à créer des mots de passe plus robustes.
Article original de Sophos France

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Cabinet de Consultants et de Formation en Informatique et Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Robustesse des mots de passes : techniques et astuces