INNOVATION & SOLUTIONS | **CYBERSÉCURITÉ** | ANALYSE
Publié le 14 décembre 2021, 16:07. Modifié le 15 décembre 2021, 09:12.

Pourquoi et comment gérer ses différents mots de passe en ligne

par Grégoire Barbey

Image d'illustration | Unsplash / Towfiqu barbhuiya

La cybercriminalité ne semble pas prendre de vacances, malgré la fin de l'année qui approche à grands pas. Dernière victime connue en date, l'entreprise immobilière DBS Group, qui possède plusieurs régies immobilières, comme l'a révélé *Le Temps*. La multiplication des cyberattaques est devenue ces derniers mois un sujet abordé quotidiennement, et est devenu un enjeu politique.

Pourquoi c'est important. Si la sécurité absolue n'existe pas, il existe pourtant des bonnes pratiques pour limiter la capacité des cybercriminels à pénétrer dans des systèmes informatiques par des moyens conventionnels. Face aux failles de sécurité type zéro-day qui peuvent potentiellement affecter une quantité de services phénoménale, la marche de manœuvre individuelle est restreinte. Mais comme le rappelait le directeur du Cyberpeace Institute, Stéphane Duguin, à *Heidi.news* en novembre, les comportements individuels qui sont comparables à des gestes barrières «permettent déjà, selon les études, de se protéger contre 80% à 99% des menaces».

Parmi ces mesures d'hygiène numérique figurent en première place… les mots de passe! Certes, la recommandation de privilégier des mots de passe robustes est répétée sans cesse comme un mantra. C'est pour une bonne raison.

Les techniques utilisées par les cybercriminels. «Pour comprendre comment choisir un bon mot de passe, il faut savoir comment les cybercriminels vont essayer de le casser», explique Steven Meyer, CEO de l'entreprise de cybersécurité ZenData. Pour craquer un mot de passe, les cybercriminels vont:

1. Essayer des mots de passe qui ont fuité et sont associés au nom d'utilisateur de l'individu ciblé. Le fondateur de Facebook, Mark Zuckerberg, s'était fait pirater ses comptes Twitter, Pinterest et Linkedin en 2016. «Il est possible que Mark Zuckerberg ait utilisé la même adresse email et le même mot de passe pour différents comptes de réseaux sociaux, permettant ainsi à ses différents comptes d'être compromis successivement», analysait alors *Tech Crunch*.
2. S'appuyer sur des dictionnaires de mots de passe qui ont fuité. En juin 2021, une liste contenant plus de 8 milliards de mots de passe a été publiée sur un forum.
3. Utiliser des variantes des mots de passe employés par la cible. «Si mon mot de passe Facebook est 1234FB, alors ils vont utiliser cette même logique pour Linkedin en essayant 1234LI», précise Steven Meyer.
4. Ajouter des informations personnelles liées à la cible: le nom des enfants, l'adresse postale, la date de naissance, le lieu de mariage, etc.
5. Recourir au «leet speak», une méthode qui consiste à remplacer certaines lettres par des caractères alphanumériques ASCII, et ajouter des préfixes et des suffixes. Exemple d'un mot de passe en «leet speak» auquel sont ajoutés un préfixe et un suffixe: password devient 123Pa$$w0rd!!!.

Et si toutes ces opérations échouent, les cybercriminels n'auront d'autre choix que d'utiliser la méthode de l'attaque par force brute qui «consiste à tester toutes les combinaisons possibles d'un mot de passe ou d'une clé pour un identifiant donné afin de se connecter au service ciblé», selon la définition de la Commission nationale de l'informatique et des libertés (CNIL). C'est d'ailleurs pour lutter contre ce type d'attaque que de nombreuses applications procèdent au blocage des comptes après un nombre défini d'échecs d'authentification pour un même identifiant. Steven Meyer:

> «L'objectif du mot de passe, c'est de respecter un certain nombre de règles qui poussera les cybercriminels à utiliser la méthode de l'attaque par force brute, parce qu'on peut mathématiquement calculer la force d'un mot de passe».

Statista a d'ailleurs créé une infographie intéressante, basée sur les données du site security.org, qui montre en combien de temps les différents types de mot de passes peuvent être découverts par un ordinateur.

Tableau des différents types de mots de passe, avec de gauche à droite: ceux qui ne contiennent que des minuscules, ceux avec au moins une majuscule, ceux avec une majuscule et un nombre, et ceux avec une majusucule, un nombre et un caractère / Illustration Statista

Les recommandations. Le site security.org met également à disposition un calculateur de robustesse des mots de passe, un bon indicateur lorsqu'on souhaite en adopter un nouveau. Des conseils pour améliorer la sécurité du mot de passe proposé sont également accessibles.

En tenant compte de ces informations, Steven Meyer recommande:

> De ne pas réutiliser un même mot de passe ou une variation de celui-ci pour différents accès;
>
> De ne pas utiliser un mot de passe évident;
>
> De ne pas mettre d'informations personnelles;
>
> De choisir un mot de passe long – de 16 caractères ou plus, selon security.org –, comprenant des lettres, des chiffres et des caractères alphanumériques.

Idéalement, il faudrait même que les lettres n'aient pas de suite logique.

Comment se rappeler de ces mots de passe? Avec la multiplication des services numériques, et en tenant compte des recommandations des professionnels de la sécurité, on peut se

retrouver des dizaines de mots de passe différents. Comment s'en rappeler? Il existe justement des gestionnaires de mots de passe.

Comme dans tous les domaines, il existe différentes offres de service, et donc des avantages et désavantages. Les gestionnaires de mots de passe peuvent prendre la forme d'un add-on lié au navigateur web ou d'une application. Ils proposent de stocker ces informations dans des coffres-forts virtuels, via un serveur cloud, ou directement sur un appareil. Les meilleurs services permettent également de déterminer la fiabilité des mots de passe, s'ils ont été réutilisés ou compromis dans une fuite de données. En général, ces services sont payants, bien qu'il existe également des versions gratuites fournissant des fonctionnalités limitées.

Apple fournit aussi son propre gestionnaire de mots de passe. Steven Meyermet en garde:

> «Il faut être vigilant, car si quelqu'un prend le contrôle de votre compte iCloud, il aura ainsi accès à tous les appareils qui lui sont reliés et tous les mots de passe. Il faut garder à l'esprit la balance bénéfices-risques.»

Les gestionnaires de mots de passe sont utiles, mais seuls, ils ne sont pas une garantie de sécurité. Les utilisateurs doivent garder à l'esprit quelques règles d'utilisation:

- S'en tenir à des mots de passe générés aléatoirement. Pour cela, il faut configurer le gestionnaire pour qu'il génère des mots de passe de 20 caractères;
- Ne pas stocker les identifiants ailleurs, ni les mettre par écrit;
- Ne pas partager les mots de passe ou les enregistrer sur des appareils partagés;
- Activer l'authentification à deux facteurs;
- Modifier immédiatement les identifiants lorsqu'ils sont compromis;
- Et ne jamais recycler d'anciens mots de passe.

Les gestionnaires de mots de passe exigent en général un mot de passe principal hors ligne pour y accéder. Ce mot de passe doit être sûr et différent des autres utilisés par le passé. Ces services ne sont pas à l'abri d'une attaque, d'où l'importance de conserver une bonne pratique dans leur utilisation. La Confédération utilise le logiciel Keepass pour son personnel, et détaille la meilleure manière de le configurer sur son site.

L'authentification à deux facteurs. Pour renforcer encore davantage la sécurité des identifiants, il faut systématiquement recourir à l'authentification à deux facteurs. Lorsqu'on se connecte à un service, celui-ci exigera une preuve supplémentaire pour être authentifié. En général, cette preuve prend la forme d'un code envoyé par SMS ou communiqué par téléphone, ou une notification sur un autre appareil. A défaut de protéger les mots de passe contre le vol, l'authentification à deux facteurs permet de limiter la capacité des cybercriminels à pénétrer dans un système dont ils auraient obtenu les identifiants.

Si aucune de ces mesures ne peut garantir une sécurité absolue, combinées, elles permettent de renforcer considérablement la protection des individus et des organisations contre les cyberattaques. Tout le monde sait que le verrou de la porte d'entrée de sa maison ou de son appartement n'est pas une garantie absolue contre les intrusions. Et pourtant, qui s'en passerait pour autant? Pour la sécurité informatique, c'est la même logique.

Cybersécurité **Cyberattaque** **Cyberespace** **Mots De Passe** **Password**