EVO NEWS

LA CYBERSÉCURITÉ

EVOLINK

EVO NEWS

CONSEILS PRATIQUES

Les mots de passe

Nous sommes contraints d'utiliser beaucoup de mots de passe. Il est important de respecter ces règles :

1) Avoir au minimum 16 caractères
2) Dédier un mot de passe pour chaque service et **pas un mot de passe pour tout**
3) Respecter certains critères de complexité

Créer des mots de passe fiables est une chose, les retenir en est un autre. Plusieurs approches existent et, actuellement, nombre de spécialistes conseillent d'utiliser des programmes qui permettent de créer des mots de passe complexes, et de les conserver de manière sécurisée. Cette approche est pleine de sens dans un environnement professionnel, où plusieurs personnes doivent avoir accès à ce type de données sensibles. Toutefois, il faut être conscient qu'en cas de perte de données au niveau de la base, ce sera bloquant et très impactant. L'utilisateur de ce type de programme doit donc être en mesure de garantir l'intégrité des données qui y sont liées, et leur sauvegarde, sans quoi il pourra tout perdre. Ce type de programme peut également être piraté et vous ne pourrez pas forcément toujours y avoir accès en cas de besoin.

Votre mémoire (humaine) ne peut être piratée. En revanche, il vous appartient de ne pas oublier votre mot de passe (il faudra tenir un registre à jour sur papier dans un lieu sûr). Le fait de mémoriser ses mots de passe peut être ennuyeux, si l'on force les changements tous les 30, 60, ou même 90 jours. Cette méthode est de moins en moins appliquée. Nous nous rendons compte que cette politique n'amène pas le niveau de sécurité souhaité. Les utilisateurs auront comme reflex de noter leurs mots de passe un peu partout, l'effort de les retenir cycliquement présente une difficulté effective.

Un autre effet était de créer des mots de passe (ou plutôt un mot de passe (pour tous ces comptes et services)) facile à se rappeler et, souvent, facile à pirater. Il semble plus raisonnable de choisir un mot de passe fort (donc long), mnémotechnique et adapté à chaque service.

Une méthode est de choisir et retenir 3 à 4 mots qui sont simples à se rappeler. Par exemple: **chocolat, pont, bon, bienvenue**

On décidera, une fois pour toutes, de mettre la première lettre des mots, ou la première lettre de chaque mot, ou la dernière, ou pourquoi pas l'avant-dernière. L'important sera de se discipliner à toujours la même logique. Puis, on va intercaler entre deux de nos mots, ou au début, ou à la fin, un élément qui identifie le compte ou le service pour lequel on utilise le mot de passe.

ChocolatWindowsPontBonBienvenue

On se retrouve maintenant avec un mot de passe de 31 caractères. Il faut encore augmenter sa complexité pour esquiver les derniers algorithmes de craquage. On peut se fendre de deux autres opérations. On décidera par exemple de substituer, systématiquement, une lettre courante par un

chiffre, par exemple la lettre «o» sera remplacé par le «0», et une autre par un caractère spécial, par exemple, la lettre «a» par «@». Notre mot de passe devient donc :

Ch0c0l@tWind0wsP0ntB0nBienvenue

Pour augmenter encore le niveau de sécurité, on pourrait décider, sur nos quatre mots de base, de choisir l'avant-dernier en allemand, et le dernier, en anglais.

Ch0c0l@tWind0wsP0ntGutWelc0me

Le fait de mêler plusieurs langues permet de mettre en difficulté certains outils de piratage travaillant avec performance sur l'unité «mot» en se basant sur un dictionnaire. Les moteurs actuels de crackage de mot de passe peuvent très rapidement tester des mots entiers en utilisant des dictionnaires. Les tests exhaustifs des possibilités pourront être fait très rapidement !

Si on utilise des mots anglais, on aura un champ lexical d'environ 200'000 mots courant (171'000), 60'000 pour le français et l'allemand. Si on mêle ces trois langues, on aura un nombre bien plus important de possibilités, donc une durée de craquage exponentiellement augmentée. Certains détracteurs de cette méthode, relèvent, avec raison que le champ lexical moyen (mots utilisés par le commun des mortels est de 200'000 mots.

Postulons, que le programme de craquage soit configuré pour exploiter que la partie courante du vocabulaire, postulant également qu'il gère les permutations « connues, @=a, e=3, o=0, etc.), un mot de passe construit selon la méthode suivante mettra, en local avec les puissances de calcul actuelles, au mieux, un peu plus de 500 ans pour être piraté si on restait sur une seule langue.

L E S A V I E Z - V O U S ?

L'assistant google vous écoute en permanence...

Lorsque votre appareil n'est pas en veille, le micro fonctionne et donne accès à toutes les informations que vous transmettez oralement. La mention « Ok Google » n'active pas ce système, mais marque le début de l'enregistrement de la séquence vocale qui sera disponible sur votre compte. Ainsi, votre téléphone est un outil permettant de vous espionner à votre insu et avec facilité.

Vous avez reçu un mail de phishing ?

Sans l'ouvrir, transférez-le à l'adresse ***reports@antiphishing.ch*** ainsi vous contribuez à lutter contre les escrocs. En reportant des tentatives de phishing, la Confédération prend des mesures afin de réduire le succès des escrocs.

L'ACTU

Nouvelle faille de sécurité sur WhatsApp, attention aux fichiers MP4 !

Un conseil ? Vérifiez que votre application soit bien à jour !

src : capital.fr

Une équipe de chercheurs révèle que la 5G présente au moins 11 failles de sécurité.

src : siecledigital.fr

Un label pour certifier la cybersécurité des PME voit le jour en Suisse

Fin 2019, le label de cybersécurité, **cyber-safe.ch,** destiné aux entreprises sera disponible. Il a été créé par des politiciens, des chercheurs et des spécialistes IT et PME à Lausanne.

src : ictjournal.ch

FREEWARE

Keepass

Keepass est un gestionnaire de mots de passe simple d'utilisation, qui permet de générer, stocker et organiser de manière structurée le stockage de ses mots de passe. Les éléments accessibles via l'interface graphique sont protégés dans une base de données cryptée.

Pour une personne sachant gérer des sauvegardes et ne désirant pas humainement mémoriser ses mots de passe, c'est un outil précieux. Toutefois, il convient de veiller à la bonne sécurité de l'ordinateur exécutant ce programme.

Pour les mots de passe utilisés en entreprise et devant être accessibles par plusieurs personnes, c'est la solution idéale.

Pour télécharger Keepass, c'est par ici : keepass.info/download.html

OUTIL

M-Files®

Pourquoi considérons-nous M-Files comme un outil incontournable d'aide à la sécurisation ?

52% des données sont des « Dark Data », c'est-à-dire des données stockées dans les systèmes et dans les référentiels, mais qui ne peuvent pas être utilisées pour la prise de décision car elles ne sont pas maîtrisées. Et par conséquent, les protéger devient impossible.

M-Files vous aide à reprendre la maîtrise de vos données et à définir un périmètre de protection adapté.

De plus, M-Files permet d'auditer les accès et de définir des permissions de manière dynamique en fonction de la nature d'un élément. Ceci de manière automatisée quand bien même la nature du document change en cours de route ! Outre ces aspects, M-Files offre une infinité de fonctionnalités qui en fait un outil incontournable de la sécurisation.

Dans notre prochain numéro, encore des informations sur la manière dont nous utilisons M-Files dans le domaine de la sécurité informatique.