OUCH! Janvier 2023

Votre bulletin mensuel sur la sensibilisation à la sécurité

Biométrie - La sécurité en toute simplicité

Aperçu

Vous détestez les mots de passe ? Vous en avez assez de vous connecter constamment à de nouveaux sites Web ou vous ne parvenez pas à vous souvenir de tous vos mots de passe complexes ? Vous êtes frustré de devoir générer de nouveaux mots de passe pour les nouveaux comptes ou de devoir changer les anciens mots de passe pour les comptes existants ? Nous avons une bonne nouvelle pour vous. Il existe une solution appelée biométrie qui permet de faciliter la cybersécurité. Nous expliquons ci-dessous ce qu'est la biométrie, comment elle vous simplifie la vie et pourquoi vous allez commencer à en voir de plus en plus.

Tout d'abord, pourquoi des mots de passe ?

Les mots de passe font partie de ce que l'on appelle l'authentification, c'est-à-dire le processus qui consiste à prouver qui vous êtes. Il y a généralement deux choses que vous pouvez fournir pour prouver votre identité : quelque chose que vous connaissez (comme vos mots de passe) et quelque chose que vous avez (comme une carte de retrait ou votre appareil mobile). Traditionnellement, l'authentification se fait par des mots de passe. Les mots de passe ont d'abord été adoptés car il s'agissait de l'une des solutions d'authentification les plus faciles à déployer. Cependant, au fil des ans, nos vies sont devenues beaucoup plus compliquées et les comptes beaucoup plus nombreux qu'on ne l'aurait imaginé. Il est assez fréquent qu'une personne ait plus de 100 mots de passe dans sa vie professionnelle et personnelle.

En outre, les cyber-attaquants sont devenus très doués pour deviner, voler ou craquer les mots de passe. C'est pourquoi il existe tant de règles concernant les mots de passe, comme la nécessité de les rendre longs (afin qu'ils soient difficiles à deviner) et d'utiliser un mot de passe unique pour chaque compte (ainsi, si l'un de vos comptes est piraté, vos autres comptes soient toujours en sécurité). Le problème de toutes ces exigences en matière de mot de passe est qu'elles rendent la cybersécurité plus difficile. Les gestionnaires de mots de passe sont d'une aide précieuse car ils mémorisent en toute sécurité tous vos mots de passe et vous connectent aux sites Web à votre place, mais existe-t-il une meilleure solution ? C'est là que la biométrie peut être utile en fournissant un troisième élément pour prouver votre identité - quelque chose que vous êtes.

La biométrie

Comme les mots de passe, les données biométriques sont un autre moyen de prouver qui vous êtes. La différence est qu'au lieu de devoir se souvenir de quelque chose (comme vos mots de passe), vous utilisez un élément de votre personnalité pour prouver votre identité, par exemple en utilisant votre empreinte digitale pour accéder à votre téléphone.

La biométrie est beaucoup plus simple, car vous n'avez pas à vous souvenir ou à taper quoi que ce soit, vous vous authentifiez simplement en utilisant qui vous êtes. Il existe de nombreux types de données biométriques, comme la voix, la démarche ou l'iris. Cependant, les empreintes digitales et la reconnaissance faciale sont les deux plus courantes, surtout pour les appareils mobiles. Si la biométrie présente un nombre considérable d'avantages, elle a aussi quelques inconvénients, l'un des plus importants étant que si votre empreinte digitale ou votre visage est copié par des cyber-attaquants, vous ne pouvez pas les changer.

Les clés d'accès

Dans les mois et années à venir, vous devriez commencer à voir la biométrie remplacer les mots de passe grâce à une nouvelle technologie appelée les clés d'accès. Cette technologie est adoptée par Microsoft, Apple et Google et vous devriez bientôt la voir adoptée par de plus en plus de sites web au fil du temps. Les clés d'accès remplacent les mots de passe en vous permettant de prouver votre identité en utilisant simplement la biométrie combinée à votre appareil mobile. Lorsque vous créez un compte sur un site web (comme Google ou Apple), au lieu de créer un mot de passe, vous enregistrez votre appareil mobile. Vous vous connectez ensuite à ce site web en vous authentifiant avec votre appareil mobile à l'aide de données biométriques, telles que votre empreinte digitale ou votre reconnaissance faciale. Le site web fait confiance à votre appareil mobile, et votre appareil mobile confirme qu'il s'agit bien de vous grâce aux données biométriques. En outre, vos données biométriques (empreinte digitale ou visage) ne sont transmises à aucun site web. Au lieu de cela, vos données biométriques sont stockées localement et en toute sécurité sur votre appareil. Il sert juste à déverrouiller les clés d'accès, une clé unique, créée pour chaque site, que votre appareil envoie au site tout en protégeant vos données biométriques. Bien qu'aucune solution ne soit parfaite, la biométrie et les solutions comme les clés d'accès peuvent vous aider à assurer votre sécurité tout en la simplifiant.

Rédacteur Invité

Le Dr Johannes Ullrich est le doyen de la recherche du collège du SANS Technology Institute. Fort de plus de 20 ans d'expérience dans le secteur, il surveille actuellement les menaces actuelles en exploitant le SANS Internet Storm Center. Il enseigne le SEC522 (sécurité des applications Web) et le SEC503 (détection des intrusions).
Twitter : @johullrich & LinkedIn : https://www.linkedin.com/in/johannesullrich/.

Ressources

Gestionnaires de mots de passe : https://www.sans.org/newsletters/ouch/password-managers/
Plus d'informations sur les clés d'accès : https://www.sans.org/blog/what-is-phishing-resistant-mfa/

Traduit pour la communauté par : Juliette Busson