L’authentification multifacteur a prouvé qu’elle fonctionne, alors qu’attendons-nous

Récemment, Amazon a annoncé qu’il exigera que tous les comptes Amazon Web Services (AWS) privilégiés utilisent l’authentification multifacteur (MFA) à partir de la mi-2024.

Nos lecteurs réguliers sauront que nous pensons que les mots de passe seuls ne sont pas une protection adéquate, surtout pas pour vos comptes importants.
Nous sommes donc tout à fait d’accord avec Amazon sur ce point.

L’authentification multifacteur est tellement plus sécurisée, et avec cela beaucoup plus indulgente, que les mots de passe seuls.
Je ne le recommanderais pas, mais écrire votre mot de passe sur un Post-It et le coller sur votre moniteur ne servira à rien à un attaquant si vous avez correctement configuré votre MFA.
Aussi non recommandé, mais vous pouvez même réutiliser votre mot de passe faible sur chaque site, tant que tous ces comptes ont été protégés avec le meilleur que MFA a à offrir.

Le dernier élément de cette phrase, « le meilleur que l’AMF a à offrir », est important. Comme Amazon l’a écrit dans son annonce :

> « Nous recommandons à tout le monde d’adopter une forme d’authentification multifacteur et encourageons en outre les clients à envisager de choisir des formes d’authentification multifacteur

> résistantes au phishing, telles que les clés de sécurité. »

Ce qu'il faut retenir ici, c'est que toutes les formes d'AMF ne sont pas aussi sûres. Lorsque vous avez le choix, la meilleure forme d'AMF est un mot de passe et une clé matérielle, mais cela signifie que vous devrez acheter une clé matérielle.
S'il vous plaît considérez dong ainsi, car ils valent le petit investissement et pas aussi intimidant qu'ils peuvent paraître.

Les clés de sécurité conformes aux normes FIDO U2F ou FIDO2/WebAuthn sont intrinsèquement résistantes aux attaques par proxy inverse et aux attaques de l'homme du milieu qui seraient en hausse en ce moment.

Si vous n'êtes pas encore prêt à franchir cette étape, la meilleure forme d'AMF utilise une application qui vous invite avec une notification sur votre téléphone.
Vient ensuite l'authentification multifacteur qui utilise un code provenant d'une application sur votre téléphone, et la version la moins bonne de l'authentification multifacteur utilise un code envoyé par SMS.

Mais même cette version la moins bonne offre une bonne partie de la sécurité.

En 2019, Alex Weinert de Microsoft a écrit que, sur la base des études de Microsoft, votre compte est plus de 99,9% moins susceptible d'être compromis si vous utilisez MFA.
Cette année (2023), Tom Burt de Microsoft a bloggé:

> « Bien que le déploiement de l'authentification multifacteur soit l'une des défenses les plus simples et les plus efficaces que les entreprises puissent déployer contre les attaques, réduisant le risque de compromission de 99,2 %, les acteurs de la menace profitent de plus en plus de la « fatigue de l'AMF » pour bombarder les utilisateurs de notifications MFA dans l'espoir qu'ils accepteront enfin et fourniront l'accès. »

Ainsi, les chiffres sont légèrement en baisse, principalement parce que les cybercriminels ont commencé à s'adapter et trouvent des moyens de contourner les méthodes MFA les plus faibles.

Une attaque par fatigue MFA, alias bombardement MFA ou spam MFA, est une stratégie d'ingénierie sociale où les attaquants déclenchent à plusieurs reprises des demandes d'authentification à deuxième facteur.
L'attaquant bombarde l'utilisateur de demandes d'autorisation d'accès et espère que la victime visée se lasse du racket ou fait une erreur et appuie sur le bouton convoité « Oui, c'est moi ».

Pourtant, un taux de réussite de plus de 99% n'est pas une mince affaire.
Et ce nombre s'améliorera avec une meilleure AMF.

Ce qui nous freine, c'est le nombre de sites et de services qui nous offrent la possibilité d'utiliser MFA.
Alors s'il vous plaît, si vous ne le faites pas, arrêtez de demander aux utilisateurs des mots de passe plus complexes qui changent toutes les quelques semaines, mais commencez à implémenter MFA pour eux.
Cela augmentera non seulement la sécurité, mais offrira également une meilleure expérience utilisateur.

À un moment donné, les utilisateurs devraient exiger et exigeront de pouvoir utiliser l'authentification multifacteur pour protéger leurs comptes contre les abus ou la prise de contrôle par des cybercriminels.
Donc, leur fournir cette option signifie que vous êtes prêt pour l'avenir.

Pour vous aider en tant qu'utilisateur à démarrer, voici des liens vers les instructions de configuration 2FA pour les cinq sites Web les plus visités:

- Vérification Google en 2 étapes
- Vérification YouTube en 2 étapes
- Authentification à deux facteurs Facebook
- Authentification à deux facteurs Twitter
- Authentification à deux facteurs Instagram

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231010
"C'est ensemble qu'on avance"