SpaceFox

Zeste de savoir

Comment casser votre double authentification et la rendre tout à fait inutile

25 avril 2023

Table des matières

Introduction

Dans mon entreprise, on a une tradition pour rappeler aux employés l'importance de ne pas laisser une session ouverte sans surveillance: si on trouve un ordinateur déverrouillé et qu'on peut le faire sans que personne ne réagisse, on envoie un message pour que le fautif (ou la fautive) offre des croissants à l'équipe.

C'est assez gentil pour ne pas vexer les gens ni leur pourrir la journée, et assez punitif pour être efficace. Et surtout c'est pédagogique: si quelqu'un peut se servir de l'ordinateur assez longtemps pour envoyer un message du type *«Je paie les croissants mardi»*, cet attaquant a aussi assez de temps pour transférer des documents privés ou se ménager une porte d'entrée discrète pour revenir plus tard en toute quiétude.

Mais ce que j'ai vu aujourd'hui était bien pire qu'une simple messagerie laissées sans surveillance.

C'était une page de connexion à un outil d'administration de machines dans le *cloud*. Déconnectée, certes, mais avec le login et le mot de passe enregistrés dans le navigateur, et la double authentification activée, ainsi qu'une icône bien particulière à côté de la barre d'URL du navigateur, celle de Authenticator .

J'appelle donc mon collègue, et:

1. entrée pour valider le formulaire login/mot de passe déjà enregistrés.
2. Un clic sur Authenticator pour l'ouvrir.
3. Un clic sur le code à usage unique pour le copier.
4. ctrl-v dans le champ de double authentification pour le copier.
5. entrée pour valider la double authentification.

Et voilà!En quelques secondes, j'avais accès à toute son administration *cloud* (donc avec possibilité de pas mal de dégâts) malgré un compte protégé par un mot de passe fort **et** une double authentification!

Pour une authentification réellement robuste

1. N'enregistrez pas votre mot de passe dans votre navigateur. Utilisez des outils dédiés (KeePassXC par exemple)

2. Le support de double authentification ne doit **jamais** être le même que celui de l'authentification principale.

Les coffre-forts de mots de passe ont souvent des durées de verrouillages courtes, et surtout se verrouillent tous seuls en même temps que la session. Comme ça, même si un petit malin a lu votre mot de passe de session derrière votre épaule, il devra *aussi* avoir votre mot de passe de coffre-fort et n'aura pas directement accès à tous vos secrets.

Et surtout, le principe même de la double authentification, c'est d'avoir une seconde source d'authentification *séparée* de la première. Alors, oui, c'est très pratique, cette extension dans le navigateur qui permet en un clic et un raccourci de remplir l'information pour se connecter au site voulu.Mais ce faisant, ça annihile tout un pan de la sécurité du système!

Ce genre d'extension devrait être réservé aux authentifications qui *ne se font pas* sur l'ordinateur où elle est installée – sur vos applications de smartphone, par exemple.

Conclusion

Icône: création personnelle, domaine public (c'est une emoji clé sur fond bleu…)