Mastodon : Les bonnes pratiques cyber Ã adopter
Internet
PostÃ© par : JulieM
PubliÃ©e le : 23/11/2022 14:00:00

Les rÃ©centes Ã©volutions de Twitter ont poussÃ© un certain nombre de ses utilisateurs Ã quitter le rÃ©seau social pour migrer vers une nouvelle plateforme, Mastodon. En apparence similaire, le rÃ©seau social fondÃ© par Eugen Rochko se distingue pourtant par son architecture open source.

Voici le dÃ©cryptage de Melissa Bischoping, SpÃ©cialiste de recherche sur la sÃ©curitÃ© des endpoints chez Tanium, qui explique les prÃ©cautions que doivent prendre les nouveaux utilisateurs de Mastodon pour Ã©voluer sur le rÃ©seau social en toute sÃ©curitÃ©.

Â« Mastodon s'est rapidement imposÃ© comme le point de chute des personnes qui ont choisi de quitter Twitter ces derniÃ¨res semaines. Le rÃ©seau social se caractÃ©rise par son organisation dÃ©centralisÃ©e et son code en open source qui prÃ©sente de nombreux avantages. EspÃ©rons que sa popularitÃ© croissante conduise Ã l'ajout de fonctionnalitÃ©s supplÃ©mentaires Ã mesure que la plateforme Ã©volue.

Cela dit, les personnes qui rejoignent Mastodon ne doivent pas considÃ©rer qu'il s'agit d'un rÃ©seau social au fonctionnement identique Ã celui de Twitter. Elles doivent Ãªtre conscientes des caractÃ©ristiques uniques du Fediverse, un ensemble de rÃ©seaux sociaux qui sâappuient sur des logiciels libres.

Chaque instance est gÃ©rÃ©e par un administrateur, qui a le contrÃ´le de l'infrastructure et des logiciels fonctionnant sur les serveurs. Cela signifie que vous faites confiance aux administrateurs pour sÃ©curiser et maintenir leur instance, ainsi que pour protÃ©ger votre compte.

Comme il s'agit souvent de petites Ã©quipes qui ne disposent pas d'un budget important ou d'une Ã©quipe de sÃ©curitÃ© informatique dÃ©diÃ©e, vous ne devez pas supposer qu'une instance est correctement sÃ©curisÃ©e ou privÃ©e.

Cela ne signifie pas que vous ne devez pas utiliser Mastodon, mais plutÃ´t que vous ne devez pas supposer que les donnÃ©es qui y sont partagÃ©es sont cryptÃ©es ou protÃ©gÃ©es contre le vol ou la saisie par les autoritÃ©s.

ConsidÃ©rez le Fediverse et toute instance de Mastodon comme un lieu de partage d'informations, de rencontre et de collaboration, de la mÃªme maniÃ¨re que lorsque vous vous trouvez dans un lieu public ou un cafÃ©. En bref, n'utilisez pas Mastodon pour envoyer des informations sensibles, personnelles ou privÃ©es que vous ne partageriez pas publiquement de toute maniÃ¨re.

En outre, Ã©tant donnÃ© le potentiel liÃ© Ã lâexploitation de vulnÃ©rabilitÃ©s, adoptez les bonnes pratiques pour la gestion de vos comptes - mots de passe uniques et authentification multifactorielle.

Enfin, de nombreuses instances ont Ã©tÃ© mises en place spÃ©cifiquement dans le but de tester la sÃ©curitÃ© et de signaler les vulnÃ©rabilitÃ©s, afin que la communautÃ© des hackers Ã©thiques et des bugs bounty puisse continuer Ã amÃ©liorer la sÃ©curitÃ© de la plateforme Ã mesure que sa popularitÃ© augmente. Â»