

25 déc. 2023 . 2 min de lecture

Protégez votre compte Office 365 contre les attaques MFA Fatigue : Urgence Sécurité !

Dernière mise à jour : 26 déc. 2023

Les attaques MFA Fatigue sont une menace croissante qui nécessite une vigilance accrue. Notre récent renforcement de la sécurité, à travers l'activation des "contextes supplémentaires" pour les requêtes MFA, vise à vous protéger contre cette forme d'attaque sophistiquée, comme partagé par Yannis SAADI, architecte SOC.

Comprendre les attaques MFA Fatigue

Les attaques MFA Fatigue visent à submerger les utilisateurs de notifications MFA, les incitant ainsi à accepter une notification frauduleuse. Face à cette menace, la réactivité et la préparation sont essentielles. Quelques contre-mesures très simples peuvent drastiquement réduire le risque d'attaque de MFA fatigue.



Que faire en cas d'attaque MFA Fatigue ?

Vérification des logs d'audit : Assurez vous de l'intégrité de votre boîte mail en examinant les logs d'audit dans Office 365 pour détecter toute activité suspecte. Si vous avez besoin d'aide pour analyser ces logs, n'hésitez pas à vous faire accompagner.

Changement de mot de passe : Si vous suspectez une attaque, changez immédiatement votre mot de passe pour éviter toute compromission. La vérification des logs d'audit o365 au préalable permet de vérifier que la boîte mail de l'utilisateur à qui nous nous apprêtons à réinitialiser le mot de passe n'est pas compromise.

Faux positifs : Soyez conscient des possibles faux positifs et adaptez vos mesures en fonction des particularités de votre environnement. Les appareils Apple tentent parfois des reconnections en "arrière-plan" qui peuvent adopter le même comportement que du MFA Fatigue. Les configurations décrites dans la partie suivante permettent de mieux distinguer ces faux positifs.

Activation des "contextes supplémentaires" dans Office 365

Pour renforcer votre sécurité :

Accédez au Portail Microsoft Entra.

Dirigez vous vers Identité > Protection > Méthodes d'authentification > Microsoft Authenticator > Configurer


Configurez les paramètres avancés pour activer :

La correspondance des numéros pour les notifications Push

L'affichage du nom de l'application dans les notifications

L'emplacement géographique dans les notifications


Microsoft Authenticator sur les applications complémentaires

 Essayez-vous de vous connecter ?

CYNA-IT
yannis.saadi@cyna-it.fr

Application
Office 365 Exchange Online

Emplacement
Normandie, France



Entrez le numéro indiqué pour vous connecter.

Entrez le numéro ici

OUI

NON, CE N'EST PAS MOI

Notification MFA après les “contextes supplémentaires”

Ensemble, renforçons notre sécurité

Ces mesures sont cruciales pour protéger vos comptes et votre environnement Office 365. Le service Exchange de Microsoft constitue très souvent la première porte d’entrée vers un SI.

N'hésitez pas à suivre ce blog et les billets techniques qui y sont régulièrement décrit pour plus d’informations sur les bonnes pratiques à adopter avec les services rependus et très souvent visés. Votre vigilance et votre collaboration sont essentielles contre ces menaces.

Article rédigé par Yannis SAADI, architecte SOC chez Cyna