Sécurité du tenant

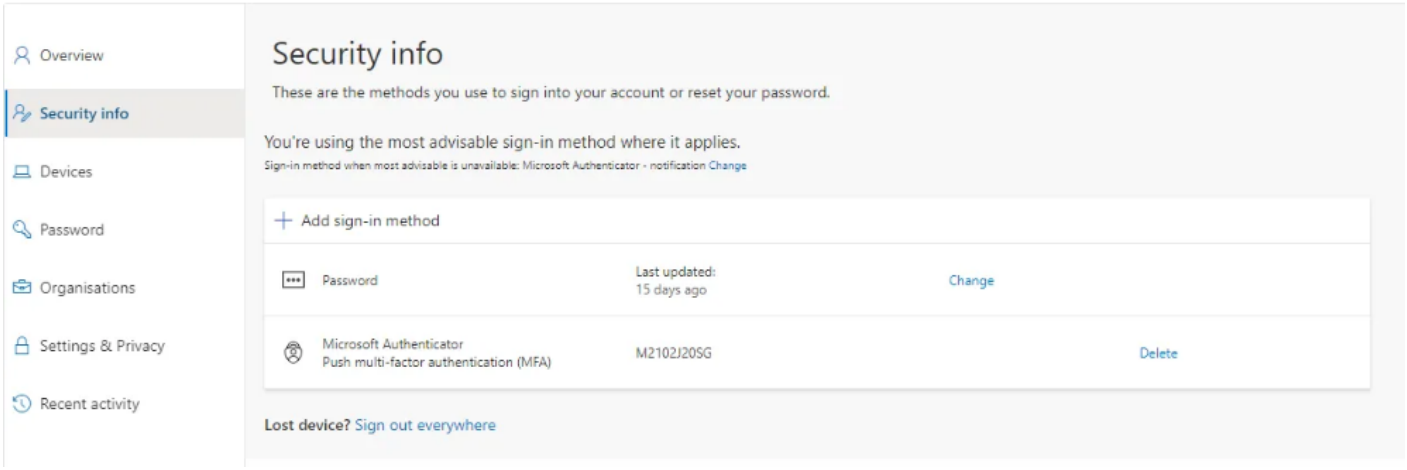
- Compte 365 compromis
- MFA
- Usurpation d’identité procédure
- Bloquer un domaine, une adresse mail du tenant
- Vérifier les règles cachées en SHELL
- Audit du tenant / Compliance
- Stratégie SSPR Microsoft

Compte 365 compromis

Connexion sur le poste de l’utilisateur

Reset du mot de passe depuis le centre d’administration O365

Depuis le compte de l’utilisateur (via le web) ⇒ déconnexion de tous les appareils



Connexion au compte Outlook de de l’utilisateur.

Vérifier que des règles (obscures) n’aient pas été appliquées.

Analyse antivirus sur le poste.

Pistes trouvées sur un site.

- Ne pas saisir de données
- Se déconnecter de l'internet
- Effectuez une analyse complète de votre machine à l'aide d'un logiciel antivirus/anti-malware.
- Changez vos mots de passe
- Assurez-vous d'avoir sauvegardé vos fichiers dans un endroit sûr.
- Supprimez le cache et les comptes supplémentaires de votre navigateur.
- Signaler un e-mail comme spam

Qu'est-ce que l'hameçonnage ?

L'**hameçonnage** est une pratique qui consiste à envoyer des courriels nuisibles aux utilisateurs d'Internet afin de les escroquer. Il s'agit d'un type d'**ingénierie sociale** où les escrocs tirent parti des aspects psychologiques des individus pour les amener à agir de manière irrationnelle. L'objectif est d'obtenir l'accès à des informations privées sur les utilisateurs, notamment des données financières, des identifiants de système, des numéros de carte de crédit, etc.

Comment fonctionne le phishing ?

Pour ce faire, un lien malveillant est inséré dans un courriel d'hameçonnage. Si vous cliquez sur ce lien, un **logiciel malveillant** infectera votre appareil et commencera à voler vos données.

Dans une **étude** réalisée en **2018** sur plus de 700 000 courriels d'hameçonnage, près de la moitié des destinataires ont ouvert le courriel et environ un tiers ont cliqué sur le lien d'hameçonnage. Alors, quels sont les problèmes qui peuvent survenir après avoir cliqué sur ce lien, et que pouvez-vous faire pour limiter les dégâts ?

PROCEDURE

1. Réinitialiser le mot de passe de l'utilisateur (si l'utilisateur est un utilisateur géré dans le nuage, sinon sur l’ad local)
2. Activer l'authentification multifactorielle
3. Révoquer tous les jetons de rafraîchissement, ce qui oblige l'utilisateur à se reconnecter. (Depuis le portail azure)
4. Désactiver les règles de transfert (encore mieux modifiez la politique antispam outbound et désactiver les transferts auto a l’extérieur pour tous)
5. Désactiver le partage anonyme de calendriers
6. Supprimer les options de transfert de boîte aux lettres

Un script existe pour faire cela en powershell :

Scripts/Remediate-BreachedAccount.ps1 at master · O365AES/Scripts · GitHub

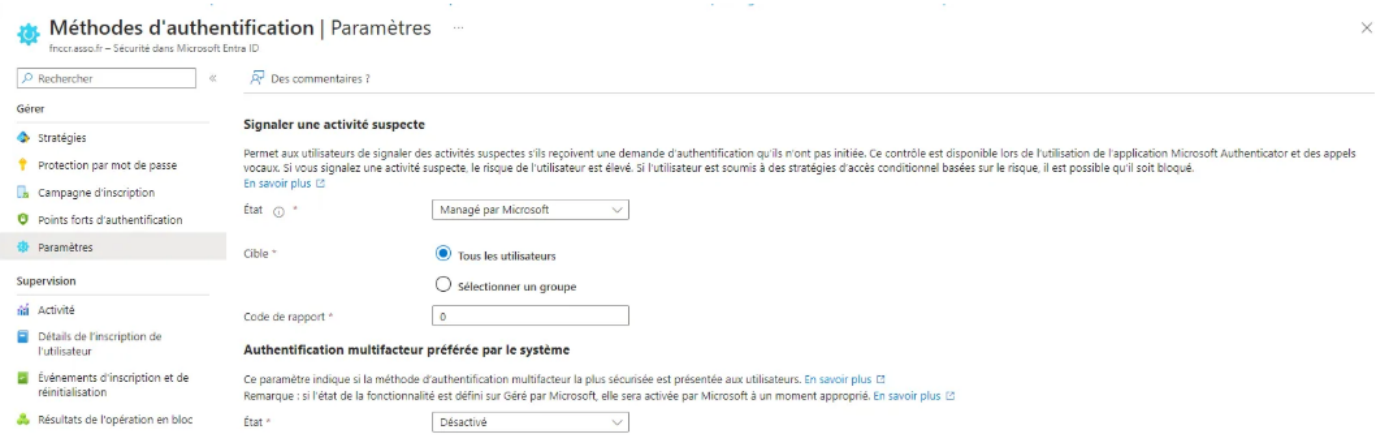
Pour plus chez Microsoft :

Réponse à un compte de messagerie compromis - Office 365 | Microsoft Learn

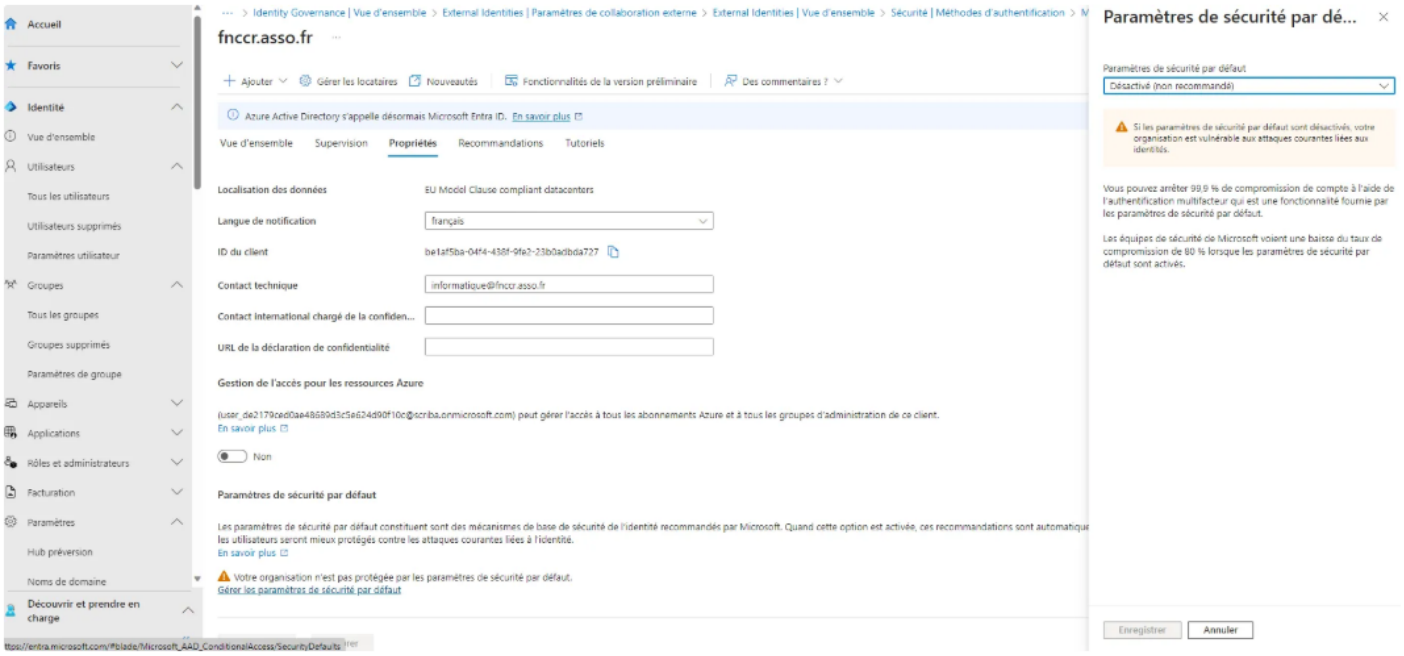
MFA

ENTRA

Méthode MFA préférée par le système



Dans vue d’ensemble



Mail type pour explication :

Bonjour Laura,

Ce mail fait suite à ma tentative infructueuse de contact.

Microsoft vous a adressé cette notification, car Microsoft va déployer sur votre tenant, des presets de sécurité par défaut pour améliorer la sécurité des comptes de votre organisation.

Ces presets vont occasionner :

- La désactivation des protocoles de connexion non sécurisés
- L'obligation, pour vos utilisateurs, de valider leurs connexions aux services 365 avec une méthode supplémentaire d'authentification. (MFA : Multi Facteur Authentification)

Pour valider leur identité lors de leurs connexions, vos utilisateurs pourront valider une notification sur une application à installer sur le mobile (Microsoft Authenticator, disponible gratuitement sur IOS et Android) ou entrer un code de sécurité qu'ils auront reçu par SMS.

Ces prochains jours, vos collaborateurs seront invités à configurer cette méthode MFA en se connectant en web sur https://office.com

A l'issue de la campagne d'inscription, toute connexion n'utilisant pas le MFA sera bloquée.

Actuellement, 58 utilisateurs sur 153 au total sont déjà prêts pour utiliser le MFA, leurs méthodes sont déjà configurées activées. Je vous invite à demander à vos collaborateurs de se connecter sur Office.com pour vérifier que tout est en ordre.

Quelles sont vos disponibilités pour échanger sur ce sujet ?

Vous pouvez me recontacter au 05 57 92 87 99 et en répondant à ce mail.

Dans l'attente de votre retour, je vous souhaite une excellente journée.

Par suite des réceptions de mails frauduleux et tentatives d'intrusions sur vos comptes Microsoft, il est impératif que seuls vos collaborateurs puissent accéder aux données 365 de votre entreprise.

L'authentification multi-facteurs, ou authentification forte, est principalement réputée pour constituer une défense supplémentaire et rendre plus difficile l'accès d'une personne non autorisée à un réseau ou à une base de données. La mise en place d'une solution MFA robuste permet de sécuriser instantanément les données et les ressources informatiques contre le vol d'identité, l'usurpation de compte et le phishing.

Les entreprises recourent donc au MFA pour contrôler l'accès à leurs systèmes et solutions informatiques internes.

Selon Microsoft, le MFA bloque plus de 99,9 % des attaques de compromission de compte. Vous entendrez souvent dire que le MFA est une composante essentielle de la sécurité. En effet, alors qu'il est relativement facile d'obtenir les informations d'identification d'un utilisateur par des attaques telles que le phishing ou credential stuffing, l'authentification forte multi-facteurs rend

quasiment impossible pour les hackers d'obtenir le second facteur d'authentification

L'authentification multifacteur (MFA) ajoute une couche de protection au processus de connexion. Pour accéder à leurs comptes ou à des applications, les utilisateurs doivent confirmer leur identité, par exemple en scannant leur empreinte ou en entrant un code reçu par téléphone. Elle ne demande pas de modifications sur les licences actuelles, pour les méthodes de base.

Nous pouvons configurer / activer le MFA (Authentification Multi Factorielle) sur vos comptes et faire en sorte qu'une connexion inhabituelle demande la saisie d'un code reçu par SMS par exemple.

https://support.microsoft.com/fr-fr/office/configurer-votre-connexion-microsoft-365-pour-l-authentification-multifacteur-ace1d096-61e5-449b-a875-58eb3d74de14

Vos utilisateurs peuvent dès à présent se connecter sur le portail Web https://aka.ms/mfasetup

Et configurer par eux-mêmes la méthode de confirmation qu'ils souhaitent. Nous pouvons également le faire à leur place, si nous disposons des numéros de mobile.

Les Méthodes disponibles :

- Utilisation du numéro de mobile pour recevoir par SMS un code à usage unique
- Installation de l'application Authenticator, disponible gratuitement sur Google Play Store ou Apple IOS Store , qui, une fois liée au compte 365, permettra de valider ou non une connexion au compte Microsoft 365. Cette Méthode permet de ne pas communiquer son numéro de mobile à Microsoft.
- Clé de sécurité FIDO2
- Windows Hello Entreprise

Une fois ce système configuré et activé, les services Microsoft demanderont de confirmer à la première connexion l'identité de l'utilisateur. Cette confirmation est à renouveler tous les 90 jours par défaut.

Je me tiens à votre disposition au 05 57 92 87 99 et en réponse à ce mail.

Dans l'attente de votre retour, je vous souhaite une excellente journée.

On peut mettre en place la MFA pour chaque connexion ou à la première connexion (définir la durée pendant laquelle la confiance est accordée).

On peut mettre en place des stratégies d'accès conditionnel

Il faut des business premium pour bénéficier d'INTUNE

On peut mettre une notification lorsque des mails viennent de l'extérieur alors qu'ils ne devraient pas (en Shell)

Office 365 – Ajouter un préfixe à l’objet et un disclaimer aux e-mails externes | IT-Connect

How To Warn users for Email Impersonation Phishing mail — LazyAdmin

Microsoft Authenticator App Not Working: 15 Tips to Fix It

Usurpation d’identité procédure

Connexion Exchange

Vérification que le même mail a été envoyé à d’autres utilisateur > phishing

Connexion aux centre d’administration O365

Déconnexion et reset du mot de passe > garder les informations

Connexion à ENTRA

Vérification des journaux de connexion

Vérifier dans les journaux les connexions interactives suspectes (depuis l'étranger, IP …)

Dans applications

On peut voir certaines application suspectes comme Perfectdata software > on peut voir les privilèges graph accordés.

Des concentrement utilisateurs peuvent être donnés > cliquer sur afficher les autorisation octroyées.

Masquer la visibilité de l’application

Application > application d’entreprise > Permettre aux utilisateurs la connexion & décocher toutes les case pour empêcher la propagation

Supprimer l’application et si impossible > script en Shell

Mise en place de la MFA dans l’ancienne interface

Utilisateur > MFA par utilisateur > activer et appliquer

Configuration avec l’utilisateur

Déconnexion des appareil mobile depuis l’OWA

Suppression des règles de courrier suspectes

Désactiver le SMTP authentifié

Sur le poste > analyse anti-virus

Bloquer un domaine, une adresse mail du tenant

Bloquer un mail

Dans la plateforme d’administration Microsoft Defender

Email & Collaboration > Policies and rules > Threat policies > Anti-Spam Policies

Anti spam Inbound policy (default)

Ajouter le domaine.

Vérifier les règles cachées en SHELL

Se connecter avec connect-exchangeonline (un accès partenaire suffit).

Get-InboxRule -Mailbox “DelegatorUserEmailaddress” -IncludeHidden

Get-InboxRule -Mailbox “DelegatorUserEmailaddress” -IncludeHidden -identity (rule identity) | ***remove-inboxrule***

Audit du tenant / Compliance

Des outils spécifique type Netwrix existent.

Sinon, on peut utiliser le centre d’administration compliance.microsoft.com > audit

On peut rechercher l’activité sur un compte utilisateur par exemple.

Stratégie SSPR Microsoft

La réinitialisation de mot de passe en libre-service (SSPR) est une fonctionnalité de Microsoft Entra qui permet aux utilisateurs de réinitialiser leurs mots de passe sans solliciter l'aide du personnel informatique. Les utilisateurs peuvent rapidement débloquer leur compte et continuer à travailler, quels que soient l'heure ou l'endroit où ils se trouvent. En permettant aux employés de débloquer leur compte eux-mêmes, votre organisation peut réduire les pertes de productivité et les coûts de support élevés liés aux problèmes de mot de passe les plus courants.

La SSPR comprend les fonctionnalités suivantes :

- Le libre-service permet aux utilisateurs finaux de réinitialiser leurs mots de passe expirés ou non, sans solliciter l'aide d'un administrateur ou du support technique.
- La réécriture du mot de passe permet de gérer les mots de passe locaux et de résoudre les problèmes de verrouillage des comptes via le cloud.
- Les rapports d'activité sur la gestion des mots de passe donnent aux administrateurs un aperçu de l'activité d'inscription et de réinitialisation des mots de passe au sein de leur organisation.

Ce guide de déploiement explique comment planifier, puis tester un déploiement de la SSPR.

Pour voir rapidement le fonctionnement de la SSPR, puis revenir en arrière afin d’examiner d’autres considérations relatives au déploiement :

Activer la réinitialisation de mot de passe en libre-service (SSPR)